State of Dedicated Short Range Communications Report

Table of Contents

Filings Expressing Concern Regarding NHTSA DSRC Mandate

- 5GAA
- 5G Americas
- Applied Information
- BMW of North America
- Broadcom
- Cato Institute
- CTIA
- Center for Democracy and Technology
- Competitive Enterprise Institute
- Electronic Frontier Foundation
- Electronic Privacy Information Center
- Fiat Chrysler Automobiles
- Mercatus Center
- Mercedes-Benz USA
- NCTA: the Internet & Television Association
- New America's Open Technology Institute, Public Knowledge, Consumer Federation of America
- Nexar
- Next Generation Mobile Networks Ltd (NGMN)
- Niskanen Center
- Qualcomm
- SecureSet
- Tesla
- Verizon
- Waymo LLC

DSRC in the News (Full Text Below)

Wireless industry urges NHTSA to reject mandates in favor of info-sharing to secure connected cars- Inside Cybersecurity- Joshua Higgins- April 20, 2017- Link unavailable

Automakers lay out cybersecurity needs for connected cars as NHTSA works on rules- Inside Cybersecurity- Joshua Higgins- April 19, 2017-- Link unavailable

Federal V2V Mandate Hits Roadblock- The Drive Magazine- Eric Brandt- April 17, 2017

Talking-Car Safety Mandate Hits Unexpected Pothole of Opposition- Bloomberg- Ryan Beene- April 17, 2017

Federal V2V mandate meets growing resistance- Automotive News- Ryan Beene (Bloomberg)- April 17, 2017

5GAA, NGMN argue for cellular, not DSRC, in NHTSA proposal- Fierce Wireless- Monica Alleven- April 17, 2017

Wi-Fi Advocates Raise Concerns on NHTSA Proposal for 5.9 GHz Band- Communications Daily- Howard Buskirk- April 14, 2017-- Link unavailable

Phase I DSRC/Wi-Fi Testing Extended With Recent Submittal of Broadcom Devices, Says FCC- Communications Daily- Dibya Sarkar- April 14, 2017-- Link unavailable

Industry weighs in on DSRC for V2V communications (Part 1)- RCR Wireless News- Kelly Hill- April 14, 2017

Industry weighs in on DSRC for V2V communications (Part 2)- RCR Wireless News- Kelly Hill- April 14, 2017

Cable Clashes With DOT Over Spectrum- Light Reading- Mari Silbey- April 13, 2017

NCTA: V2V Proposal Is Straying Into FCC's Lane- Broadcasting & Cable- John Eggerton- April 12, 2017

Former DHS official says connected-car network needs cybersecurity framework- Inside Cybersecurity- Joshua Higgins- April 4, 2017-- Link unavailable

Securing our intelligent, interconnected vehicles- Tech Writers Bureau- William Jackson- March 31, 2017

Cyber Issues Must Be Addressed Before DSRC is Launched, Report Says- TR Daily- Paul Kirby- March 30, 2017-- Link unavailable

Op-Eds, Blog Posts, and Third Party Statements

Straight Talk on the "Talking Car" Mandate - Real Clear Future - Marc Scribner - May 23, 2017

Danger Ahead: The Government's Plan for Vehicle-to-Vehicle Communication Threatens Privacy, Security, and Common Sense - EFF - Jamie Williams - May 8, 2017

Senseless Government Rules Could Cripple the Robo-Car Revolution - Wired - Ryan Hagemann - May 1, 2017

5GAA Submitted Comments to the National Highway Traffic Safety Administration - Yahoo Finance (from PR Newswire)- April 18, 2017

The Department of Transportation's Proposed Vehicle-to-Vehicle Technology Mandate Is Unprecedented and Hasty- Mercatus Center Blog - Brent Skorup- April 14, 2017

Serious Privacy Risks Lie in the Path of Vehicle Automation- Center for Democracy and Technology Blog- Joseph Lorenzo Hall- April 13, 2017

Proceed With Caution- Morning Consult- Alex Kreilein- April 12, 2017

Public Knowledge Files NHTSA Comments Raising Safety, Privacy Concerns with DSRC Technology- Public Knowledge Blog- Shiva Stella- April 12, 2017

CEI Submits Comments on Proposed Vehicle-to-Vehicle Communications Mandate- Competitive Enterprise Institute Blog- April 12, 2017

Protect Your Privacy and Save Money by Telling NHTSA No to the Vehicle-to-Vehicle Communications Mandate- CATO at Liberty (from the CATO Institute)- Randal O'Toole- April 5, 2017

Full Text - DSRC in the News

Wireless industry urges NHTSA to reject mandates in favor of info-sharing to secure connected cars
Inside Cybersecurity
Joshua Higgins
April 20, 2017

A major wireless industry group is urging the National Highway Traffic Safety Administration to scrap proposed mandates on securing connected cars in favor of a collaborative approach to sharing information about cyber threats.

CTIA—The Wireless Association said in comments on NHTSA's proposed rulemaking on vehicle-to-vehicle "V2V" communications that wireless networks provide "necessary data security and privacy protections necessary to play a key role in V2V communications."
"As in other sectors of the economy, NHTSA should rely on industry collaboration and information sharing to address cybersecurity and privacy concerns, in contrast to prescriptive government mandates," according to the group.

NHTSA last week closed a public comment period on the proposed rule, which would mandate automakers to install V2V communications devices in vehicles to allow safety information to be transmitted between vehicles and roadway infrastructure. The NHTSA proposal would create a "security credential management system" that would maintain the integrity and security of vehicle data.

CTIA encourages NHTSA to leverage authentication technology from commercial wireless services to secure the SCMS.

"Creating an authentication infrastructure leveraging existing commercial wireless services would reduce costs, expedite deployment, and further interoperability," CTIA writes.

The wireless association also urges NHTSA to employ security standards that are compatible with global cybersecurity standards.

"The security standards eventually adopted for the V2V SCMS should be compatible with similar global standards to ensure that automobile manufacturers and their connectivity partners can use the same SCMS protocols across the globe, as well as across sectors," the group states.
CTIA says a "technology-agnostic" approach to V2V authentication and encryption is needed to ensure global applicability of security controls for V2V communications.

"Adopting a technology-agnostic approach to V2V authentication and encryption as part of the SCMS would ensure secure communications and global applicability, as well as avoid locking the V2V SCMS into potentially dated technology," CTIA says.

CTIA's comments track with the auto industry's comments on security of V2V. However, CTIA says the SCMS should be privately managed, underscoring the wireless industry's willingness to work with automakers and the government to deliver reliable and secure V2V communications.
"The wireless industry stands ready to work with its automotive partners to ensure the delivery of reliable and secure V2V communications, increasing traffic safety and efficiency on our nation's roads and highways," CTIA states.

Automaker associations, on the other hand, have urged NHTSA to establish a government leadership role in the SCMS, with some components being managed through public-private partnerships.

While NHTSA has closed its public comment on the proposed rule, the regulator has not issued a timeline for putting forth a final rule on V2V. NHTSA has, however, collaborated with the Federal Trade Commission on hosting a workshop on connected car security and privacy later this year.

Automakers lay out cybersecurity needs for connected cars as NHTSA works on rules
Inside Cybersecurity
Joshua Higgins
April 19, 2017

The automotive industry is urging the federal government to lead on the creation of a cybersecurity credential management system to protect connected-car communications while developing a long-term strategy to establish a "scalable, nationwide, and sustainable security solution" for connected cars, according to comments submitted to the National Highway Traffic Safety Administration.

NHTSA has proposed a rule to require "vehicle-to-vehicle communications" devices in new vehicles, citing the safety benefits connected cars can provide. NHTSA closed its public comment period on the rule on April 12. The administration has not yet issued a timeline for finalizing the rule.

The industry has supported NHTSA's effort on the matter.

In comments to NHTSA the Association of Global Automakers stressed that NHTSA should include measures in the final rule to "promote and strengthen the long-term security and privacy of V2V communications."

Quick implementation of a "back office" security system to maintain integrity of communications is critical for implementation of V2V, according to the Global Automakers, stressing that the "fundamental necessities" of a security credential management system – SCMS – need to be in place for deployment.

However, the association says all features won't be necessary in the beginning, such as misbehavior detection reporting features.

"While there is a fully functioning security system in place today to support pilot deployments and early adopters, Global Automakers urges DOT to define the long-term pathway towards a scalable, nationwide, and sustainable security solution," the association states. "Global Automakers stands ready to work with DOT and the industry to make this happen and does not believe that this concern should delay promulgation of the V2V [Federal Motor Vehicle Safety Standard]."

Global Automakers says the federal government should take a leadership role in standing up the security management system and provide the necessary oversight to ensure trust and interoperability within the V2V ecosystem.

The Alliance of Automobile Manufacturers in its comments also calls for federal leadership in creating and managing the SCMS for connected cars.

"It remains the Alliance's position that management of the central portions of the SCMS (e.g. SCMS Manager, Misbehavior authority) should be the role of the Federal government, with certain aspects run through public/private partnerships," the Auto Alliance states.

The Alliance adds that "critical security and trust features" of the SCMS must be in place well before the effective date of the rule requiring automakers to install V2V devices in their products.
In addition to outlining the needs for the SCMS, Global Automakers also urges NHTSA to avoid outlining a particular method for conducting over-the-air security updates, rather allowing flexibility by specifying requirements for updating the system without "specific approaches or technologies."

"For security software updates, such as the need for additional certificates, the vehicle would need to receive such updates in a timely manner or risk being removed from the safety network, at which point some type of malfunction indicator may need to be provided to the consumer," Global Automakers states.

Global Automakers also urges auto manufacturers to "take additional security steps such as isolation of safety-critical control systems, adopting intrusion detection measures, and implementing real-time response methods." However, the association warns that it is premature to require any other cybersecurity requirements in the V2V rule.

Federal V2V Mandate Hits Roadblock
The Drive
Eric Brandt
April 17, 2017

Vehicle-to-vehicle (V2V) technology is in a difficult spot. While the Obama-era National Highway Traffic Safety Administration came up with a proposal to mandate V2V technology in new cars, a new NHTSA leader has yet to be nominated.

The idea is to equip every new car on the road with dedicated short-range communications tech so vehicles can talk with each other to prevent accidents, among other uses. This would work with existing safety tech like automatic braking and adaptive cruise control. Believe it or not, everyone has an opinion about it.

There aren't really any party lines on this issue, and even automakers can't see eye-to-eye. While everyone seems to agree that the idea is good, not everyone agrees on how it should be implemented.

Proponents of the mandate like it because of the obvious safety benefits. (One thing everyone agrees on is that fewer accidents and traffic deaths would be a good thing.) The Association of Global Automakers, which includes Toyota and Honda, supports the proposal, and points out that over $1 billion has already been invested in V2V systems.

GM is a staunch defender of the mandate, but the Alliance of Automobile Manufacturers of which they're a member (along with Ford, Volkswagen, and many others) has some critiques. Their main complaint with the mandate is its failure to address security. Tesla has a similar gripe, saying the NHTSA strategy falls short in protection and privacy of the messages being communicated between cars.

It remains to see how this will play out. With an administration that's determined to cut back on regulations, this could get scrapped entirely—or, its popular safety benefits could help push it through.

Talking-Car Safety Mandate Hits Unexpected Pothole of Opposition
Bloomberg and Automotive News
Ryan Beene
April 17, 2017

A once-popular idea to equip cars with technology to communicate with one another and avoid collisions is encountering unexpected potholes in Washington.

An array of forces, from free-market groups opposed to government mandates to cable providers angling for greater access to high-speed wireless airwaves, have mounted opposition to a proposal that all new cars have vehicle-to-vehicle communications systems.

"This technology faces a huge number of hurdles, not the least of which is whether it's even needed," said Mike Ramsey, an analyst with the technology research firm Gartner Inc. "There are a number of reasons why it may never get off the ground."

The Obama administration proposed the rule in December, saying it could eliminate 80 percent of vehicle crashes involving unimpaired drivers. If the rule is finalized, all new light-duty vehicles would be required within four years to be equipped with vehicle-to-vehicle communication systems. The technology will work hand-in-hand with new automated safety devices, such as automatic braking, in another step toward making driverless vehicles a reality, the Department of Transportation said at the time.

More than 400 people and organizations filed formal opinions with the National Highway Traffic Safety Administration by last week's deadline, reflecting a wide range of viewpoints.

The proposal enjoys broad support from safety advocates, with the National Safety Council commenting that the technology adds a layer of awareness and redundancy to on-board vehicle sensors "that will be critical as higher levels of automation are deployed."

But automakers are split on the virtues of the plan, with some voicing strong support and others pointing out flaws in the government's approach.

The Association of Global Automakers, a trade group that represents foreign-owned automakers including Toyota Motor Corp., Honda Motor Co. and Hyundai Motor Co., says that more than $1 billion in private and public funds have been spent developing the systems. The group says the mandate is "the best way to ensure nationwide deployment" as soon as possible, according to its filing with NHTSA.

Major automotive industry companies, including General Motors, Denso Corp., Delphi Automotive and Toyota, have spent more than a decade developing vehicle-to-vehicle, or"V2V," communications systems.

"The safety benefit of V2V is undeniable. It will save lives, and everybody knows that," said Harry Lightsey, executive director of federal affairs for connected cars at GM. "A delay in rolling out V2V will cost lives, and that's a tragedy."

GM, One of the mandate's loudest cheerleaders, earlier this year launched the first V2V-equipped vehicle, the 2017 Cadillac CTS. NHTSA's proposed mandate is the best way to quickly advance the technology and to put a dent in the number of car crashes, Lightsey said.

The Alliance of Automobile Manufacturers, which represents a dozen automakers, including GM, Ford Motor Co. and Volkswagen AG, said NHTSA's proposal needed additional clarity on several issues, including how security would be addressed, and asked for more time to implement the mandate than the proposal provides.

In its comment, Tesla Inc. said policy guidance and industry cooperation would be a better approach for encouraging V2V, calling NHTSA's V2V strategy "too antiquated and vague" to protect the privacy of V2V messages.

Those messages are sent between cars 10 times per second using "dedicated short range communications" on airwaves reserved by the Federal Communications Commission in 1999.

Alternative systems

BMW AG says the proposal would require automakers to use those airwaves to comply with the rule, even as alternative systems using cellular networks emerge. In its comment, the automaker urged NHTSA to take a technology-neutral approach, saying "many of the shortcomings of DSRC can be efficiently and cost effectively addressed" using cellular-based systems.

One company offering such as system is Israel-based startup Nexar Ltd. It began operating a smartphone app-based V2V network in New York City that now includes about 2,500 vehicles, CEO Eran Shir said. Data collected from the phone's camera, GPS and internal gyroscope are analyzed in Nexar's cloud system to warn drivers of impending collisions.

Shir says that NHTSA's mandate would put cellular-based V2V technology like Nexar's at a disadvantage because companies would prioritize investments to comply with the rule.

"I would totally understand if NHTSA said, 'We're interested in safety and we want these safety features,'" Shir said. "There are millions of lives at stake. What I think is less reasonable is if NHTSA comes and says we want to regulate the technology. That doesn't make sense."

Old technology

The failure to consider alternative technologies is a significant shortcoming of the proposal, says Marc Scribner, a senior fellow at the Competitive Enterprise Institute, who co-authored a letter with four other free-market advocacy groups asking regulators to suspend the proceeding.

"You're betting on something that at its core is 10-year-old technology that isn't going to have much of a difference on safety for 20 years," Scribner said. "By the time it's effective it will be out of date by 30 years."

The Internet and Television Association, the primary cable industry trade group, criticized the proposal for overstepping NHTSA's authority by seeking to indirectly influence wireless spectrum policy overseen by the Federal Communications Commission. That agency is studying how vehicles and other Wi-Fi-enabled devices could share airwaves amid a lobbying push by cable and tech companies hungry for additional wireless bandwidth.

"NHTSA proposes to race to impose new regulations without developing a full record on alternatives, all in the hopes of narrowing the regulatory options available to the FCC," the cable group said.

Whether the proposal advances is now up to the Trump administration, which has erected hurdles to new regulations, including issuing an executive order requiring the cost of new rules be offset by savings from repealing others. The administration also hasn't nominated a leader for NHTSA, the Transportation Department agency responsible for the rule.

Transportation Department spokeswoman Allison Moore said the proposed rule is still under "careful review," adding that "all views will be considered in the decision-making process."

5GAA, NGMN argue for cellular, not DSRC, in NHTSA proposal
Fierce Wireless
Monica Alleven
April 17, 2017

Out with the old, in with the new, according to several cellular industry groups commenting on the U.S. National Highway Traffic Safety Administration (NHTSA) plan to use dedicated short-range communications (DSRC) to improve road safety.

The deadline was April 13 for the public to comment on the NHTSA's plan, which proposes requiring vehicle-to-vehicle devices to "speak the same language" through standardized messaging and would require automakers to include V2V technologies in all new light-duty vehicles. Designating a single language would solve the problem of dueling protocols, but opponents argue that DSRC is already

outdated and shouldn't be mandated. In fact, many commenters don't want to see any specific technology mandated at all.

The 5GAA, whose founding members include Ericsson, Intel, Huawei, Nokia, Qualcomm, Audi, BMW Group and Daimler AG, prefers Cellular Vehicle-to-Everything (Cellular-V2X) for V2V safety, saying it exceeds the capabilities of DSRC on more than one front. But 5GAA doesn't want to see any technology mandated.

"Rather than moving forward with the proposed regulation, NHTSA should instead undertake an updated, comprehensive technology neutral analysis of V2V solutions, including DSRC and Cellular-V2X, against the performance requirements in the NPRM," 5GAA wrote. "Consistent with a technology neutral guiding principle, any such regulation should not require one-way interoperability with a specific technology, or in any way pick technology winners and losers."

Next Generation Mobile Networks (NGMN), whose U.S. board members include AT&T, Sprint, T-Mobile, US Cellular, Verizon and Ligado Networks, commented in much the same vein, saying its V2X Task Force recommends the U.S. Department of Transportation (DoT) be technology neutral in the rulemaking. Cellular technologies beginning with 3GPP Release 14 could offer a technical and market-driven solution with a clear evolution path, they say.

NGMN recognizes the efforts taken over the past 10 years to develop and test use cases based on DSRC technology, but it notes that cellular-based communication technology has already been widely deployed within vehicles, not only for information and entertainment purposes but also for maintaining and increasing safety and security.

In its remarks, CTIA also disputes the NHTSA's assessment of the reliability of cellular networks for vehicle-based communications, noting that LTE latency rates are roughly 10 milliseconds over the air and 5G latency rates will be even lower, targeted to be five to 10 times lower.

"5G is not aspirational," CTIA wrote, adding that the FCC itself declared the deployment of 5G by as early as 2020 as a national priority. Since 5G infrastructure, particularly small cell sites and fiber, will be built close to roadways, it will be readily available to support the full range of V2V and vehicle-to-infrastructure (V2I) communications at low latency, especially in high-density areas with great demands for data throughput from a large number of users, the organization said.

5G Americas says DSRC relies on roadside units that are not ubiquitously deployed in the U.S., whereas cellular networks are ubiquitous, including in most rural areas. "At the physical layer, DSRC has several inefficiencies due to the asynchronous nature of the system, resulting in reduced range, robustness and reliability and high latency," said 5G Americas President Chris Pearson in a filing. "Currently there is no activity in the IEEE 802.11 standards body to study a next-generation DSRC technology that will meet the requirements of more advanced V2X use cases such as automated vehicles."

Cellular networks could be used to provide backhaul to the roadside units and can extend the V2X range from the 300 meters that DSRC offers to several kilometers or more, providing earlier notifications to drivers and their vehicles, 5G Americas said.

“A voluntary path to enhance the long-term safety of U.S. roadways is preferable to mandating decades’ old technology that is not likely to evolve, and therefore might not deliver benefits comparable to C-V2X,” Pearson concluded.

The NHTSA has said it will review the submitted comments and adjust its proposal as appropriate before issuing a final rule.

Wi-Fi Advocates Raise Concerns on NHTSA Proposal for 5.9 GHz Band
Communications Daily
Howard Buskirk
April 14, 2017

Industry groups and companies, eager to gain access to the 5.9 GHz band for Wi-Fi, raised concerns about a National Highway Traffic Safety Administration rulemaking notice on dedicated short-range communications (DSRC) technology and other vehicle-to-vehicle (V2V) communications. But auto industry commenters said the technologies that would be allowed as a result of new rules are critical to public safety. Public interest and free-market groups were on the same page on the 5.9 GHz issue. There was speculation early in the Trump administration the White House might kill the rulemaking (see 1612130050), released in December in the late days of the Obama presidency. Comments were posted in docket NHTSA-2016-0126.

“The Department of Transportation should quickly determine how many DSRC channels are needed for V2V and other time-sensitive safety communications and then let the FCC do its job to facilitate sharing of the remainder of the band with Wi-Fi users for commercial and safety-related but not time-critical applications,” said Michael Calabrese, director of the Wireless Future Program at New America. “Our comments conclude that separating the two or three DSRC channels needed for real-time safety signaling, while sharing the remaining channels with Wi-Fi, strikes the best balance between the public’s interest in both crash avoidance and faster, more affordable broadband connectivity.” Calabrese also told us NHTSA’s proposed plan would require all V2V signaling to occur on a single, dedicated DSRC channel of 10 MHz. Calabrese said FCC action is unlikely before the Office of Engineering and Technology wraps up the current round of interference tests.

Ajit Pai, before being named FCC chairman, supported opening up the 5.9 GHz band to unlicensed use, said Roger Entner, analyst at Recon Analytics. "I don't see any obvious reasons why Chairman Pai would reconsider his position."

The 5.9 band “is one of many issues that has been languishing at the FCC for too many years,” said Richard Bennett, network architect and free-market blogger. “Several years ago, Qualcomm proposed a resolution that would enable automakers and Wi-Fi users to get what they need. At the time, the proposal was thought to be too late but years have passed with no action from the FCC. Clearing the docket of issues that have been gathering dust should be a priority.”

“Vehicle connectivity promises to play an important and integrated role in crash prevention and easing traffic congestion, and that can result in improved safety and mobility as well as reduced greenhouse gas emissions,” the Auto Alliance said in a statement. The alliance urged NHTSA to release a Supplemental NPRM allowing automakers to provide further comment. “This SNPRM should include more specifics than the current proposal on critical topics including test criteria and the Security Credential Management System,” the group said.

"As vehicles become more connected and automated, it is important that the policy environment support the deployment of this lifesaving technology," said John Bozzella, president of Global Automakers, in a statement. "This is smart regulation that will make our roadways safer and create a competitive marketplace for further safety applications. … Our roads will be shared by various levels of automated and conventional vehicles. V2V and the safety spectrum are the code that will connect this network and ensure vehicles can communicate in the same language without interference." An FCC official and others also discussed V2V at a separate event Thursday (see 1704130019).

Groups representing automakers and others in the transportation sphere filed comments through the Safety Spectrum Coalition. "The advancements represented by DSRC are especially timely and important," the coalition said. "Preliminary 2016 data from the National Safety Council estimates that as many as 40,000 people died as a result of motor vehicle crashes last year. That marks a 14 percent increase over 2014, the most dramatic two-year escalation since 1964." The proposed rule "provides the regulatory framework and certainty necessary to drive not only substantial and rapid light-duty fleet deployment of V2V technology, but also spur innovation, competition, and deployment in the aftermarket and infrastructure industries to bring even further safety benefits to our roads," the coalition said.

Public Knowledge, New America's Open Technology Institute and Consumer Federation of America said DSRC as proposed in the NPRM raises big privacy and security issues that are never addressed. The risks grow if the spectrum is used for commercial purposes rather just for safety, the groups said. "Real-time V2V safety-of-life applications are inherently narrowband and designed to require only a fraction of the 75 megahertz of spectrum currently allocated for [intelligent transportation] and DSRC technology," the filing said.

"The 5.9 GHz band is critical to next-generation wireless broadband. Unfortunately, the NPRM engages in faulty analysis to arrive at a misguided proposal that would threaten a critical part of the country's wireless future," NCTA commented. "NCTA therefore urges NHTSA to (1) amend its cost-benefit analysis to properly account for the costs its mandate would impose on broadband consumers and investors; and (2) consider how it can advance vehicle safety while supporting the Federal Communications Commission's (FCC) efforts to permit efficient, shared use of the 5.9 GHz band."

The Competitive Enterprise Institute said NHTSA puts far too much emphasis on DSRC and the deployment of roadside equipment (RSE). "At a time where state and local transportation infrastructure facilities face large maintenance backlogs, approaching reconstruction needs, and uncertain funding, NHTSA's failure to adequately consider fiscal burdens in its analysis of alternatives is troubling," CEI commented. "Further, questions remain as to NHTSA's authority to even regulate the public RSE network." Many past auto safety mandates such as seat belts, air bags, and backup cameras "involved ideas for which there were no other obvious alternatives on the horizon," the Cato Institute wrote. "While they may or may not have been cost-effective, they at least had the virtue of not forestalling new and better technologies. The V2V mandate doesn't have that virtue."

Phase I DSRC/Wi-Fi Testing Extended With Recent Submittal of Broadcom Devices, Says FCC
Communications Daily
Dibya Sarkar
April 14, 2017

Broadcom late last week submitted prototype devices to the FCC, further extending the agency's Phase I lab testing of spectrum sharing between unlicensed Wi-Fi and dedicated short-range communications (DSRC) systems that would be used for automotive systems, said Julius Knapp, chief of the Office of Engineering and Technology. He spoke Thursday at an event hosted by Association of Unmanned Vehicle Systems International's DC chapter. Commenters to another agency also debated DSRC over vehicle to vehicle communications (see 1704130045).

Knapp said he couldn't say when Phase I will be completed because testers at FCC's Columbia, Maryland, lab will have to familiarize themselves with the newly submitted devices, how they operate and what exactly do they do. Initially, the target to complete Phase I was in January, he told us. Plus, he said during the discussion, even after tests are completed, testers may find something isn't working right and have to test again. Cooley attorney Anne Swanson, who moderated the discussion, asked whether the testing will be completed this year. Knapp replied: "I certainly hope so. I can't imagine it's going to be that long."

About a month ago, Knapp speaking at another event indicated Phase I testing was nearing completion (see 1703090041). But he said Thursday the agency later expected Broadcom would submit other prototypes so the agency could fully evaluate the sharing techniques. He said Phase I testing is divided into three parts: characterizing the radio signals the devices transmit; interference testing and mitigation techniques, meaning how the devices share without interference. Phase II will include field testing and the third phase will look at real-world testing. Most of the testing has been done with other sample devices submitted by Cisco, Qualcomm, KEA Technologies, Broadcom and CAV, Knapp said, and the FCC is analyzing the data. He said the agency plans to issue a public report at end of the Phase I.

Automakers want to use the licensed DSRC within the 5.9 GHz band for vehicle-to-vehicle and other technologies for safety and other applications, but Wi-Fi advocates want to share the spectrum (see 1702210060). The FCC is testing whether that's feasible without interfering with DSRC. There are two competing approaches -- one from Cisco and another from Qualcomm (see 1702030043) -- for how best to further reduce interference. Automakers said Qualcomm's proposal pushing for "rechannelization" would take too long. Knapp said one of the questions the FCC is trying to figure out in the testing is what constitutes "harmful interference."

Kevin Gay, chief-Intelligent Transportation Systems Policy, Architecture and Knowledge Transfer group at the Federal Highway Administration, said the U.S. transportation system is facing threats from individual attackers, criminal organizations and nation states with a goal to disrupt systems or steal intellectual property. They can penetrate a vehicle through physical ports or infotainment systems, wirelessly or through a driver's cellphone or an insurance company's device designed to gauge a motorist's driving performance, he said. Several initiatives exist to improve cybersecurity of automobiles, including the National Highway Traffic Safety Administration's best practices released last year and similar offerings from the Automotive Information Sharing and Analysis Center, he added. NHTSA was the agency receiving the DSRC and V2V comments.

Within the DSRC environment are specific security and privacy challenges, Gay said. Since 2015, his agency has been working with auto manufacturers and others to develop a prototype "security credential management system" with testing just starting now, he said. When a vehicle sends a DSRC message over the air, the system attaches a digital signature and certificate. "The intent is that any vehicle that receives that can verify the digital signature and ensure the message came from a trusted

source" rather than from someone sending "rogue" DSRC messages. He said the testing the system will help stakeholders understand challenges, eventually leading to a national system.

But Gay said the intent is not to attach one single certificate to a vehicle or an ID to a broadcasting device so no specific vehicle or device can be tracked. Instead, the system "rotates those key identifiers and provides new credentials on a weekly basis" allowing vehicles to change them frequently.

Steven Bayless, vice president-regulatory affairs and public policy, Intelligent Transportation Society of America, said his organization submitted comments to NHTSA's proposed rulemaking on a V2V safety standard. He said V2V lays the foundation for creating vehicle-to-vehicle communications platform. He said ensuring the system is secure and interoperable is vital.

Industry weighs in on DSRC for V2V communications (Part 1)
RCR Wireless News
Kelly Hill
April 14, 2017

Rulemaking comments for DSRC for V2V include potential for use of cellular-V2X, sharing of DSRC spectrum

As the cellular industry and standards bodies increasingly seek to support connected vehicles, the federal government is considering whether to mandate the use of Dedicated Short-Range Communications capabilities — or interoperability with DSRC — in all new light vehicles. The public comment period for the National Highway Transportation Safety Administration's proposed Federal Motor Vehicle Safety Standard (FMVSS) rulemaking closed this week.

The NHTSA said in the proposed rulemaking that it "believes that [vehicle-to-vehicle communication] has the potential to revolutionize motor vehicle safety. ... The agency believes that V2V will be able to address crashes that cannot be prevented by current in-vehicle camera and sensor-based technologies ("vehicle-resident" technologies). This is because V2V would employ omnidirectional radio signals that provide 360 degree coverage along with offering the ability to "see" around corners and "see" through other vehicles. ... As another source of information about the driving environment, moreover, the agency also believes that V2V can be fused with existing radar- and camera-based systems to provide even greater crash avoidance capability than either approach alone."

The NHTSA added that it believes a mandate for V2V communications is necessary in order to achieve a workable market and mass coverage for V2V and that it proposed to "standardize the content, initialization time, and transmission characteristics of the Basic Safety Message (BSM) regardless of the V2V communication technology potentially used." The proposed rulemaking outlined a timeframe in which a final rule on the subject would be made in 2019, a phase-in period would begin in 2021 and compliance would be required by 2023.

Private citizen comments on the topic consisted largely of opposition to increased radio frequency exposure and the inability to opt out of a vehicle equipped with RF communications if a mandate for V2V were to be adopted.

Below are selected excerpts from telecom and transportation companies and organizations on the National Proposed Rulemaking:

AT&T: AT&T supports the intent of the rulemaking to promote public safety, and believes that the NPRM has sought to strike a balance between setting a target for spurring the widespread deployment of a V2V capability to drive vehicle safety improvements while still leaving room for innovation and competition in the marketplace....

AT&T takes no position at this time on the specific wireless technology to be used for the communication between vehicles—i.e. the transmission of the Basic Safety Message (BSM)—in the context of the proposed mandate. Given the extensive development and market readiness of DSRC-based communications, the DSRC technology appears to be a viable means of achieving many of NHTSA's near term safety objectives. Nevertheless ... there are other rapidly emerging 3GPP-based technology, including [cellular]-V2X standards ... defined in 3GPP Release 14,11 that may offer improved radio access technology performance relative to DSRC and that in turn may offer both relatively greater safety benefits and relatively greater longevity and scalability. Although the nascence of this technology obviously challenges NHTSA's ability to fully assess it now, it is clear it will be market ready in approximately the same time frame contemplated in the NPRM for deployment of a V2V capability. Accordingly, the final rule should be careful not to foreclose continued research and development into that technology—or, for that matter, any other technologies that will be supportive of NHTSA's safety goals.

Verizon: As NHTSA moves forward with requirements for V2V, it should craft open performance requirements for V2V solutions, rather than limit the types of communications systems that might be used to meet those requirements. By focusing on system performance specifications and requiring interoperability, NHTSA will encourage developers and providers to collaborate and innovate towards efficient and safe next-generation V2V capabilities. Some of these solutions may in fact be DSRC driven. But NHSTA should not prescribe specific technology that must be deployed to meet its proposed mandate, since limiting possible solutions to a specific type of spectrum or technology will unnecessarily hamstring innovation and slow down development of potential safety improvements. As long as a proposed solution is both interoperable with other V2Vsystems and meets the specifications NHTSA eventually adopts, there is no reason to limit the technology that transmits the messaging between vehicles or between a vehicle and infrastructure. ...

Given the long runway for widespread adoption of V2V systems, a more flexible approach will prevent V2V systems from being permanently fossilized in 2017. At this early stage in development, the industry may not yet be ready to make a one-time, final determination about which technology is best-suited for a particular purpose for the next twenty-plus years. A flexible policy regarding the types of technology used for V2V will allow V2V efforts to reach their greatest potential. If only DSRC is permitted, the capabilities of V2V technology will always be confined to only what DSRC can do.

General Motors: GM believes that the NPRM's proposed lead-time and phase-in are too aggressive. This is especially true given the amount of remaining open issues and the extensive vehicle integration required to develop V2V systems. FMVSS 150 is among the most far reaching and complex rules attempted in ground vehicle transportation. As we point out in these comments, parts of the proposed rule need updates and changes. These changes in turn may lead to updates in the applicable standards. And manufacturers will need time to interpret and implement these updates, as will their suppliers and other technology partners. These will include significant activities for vehicle, production control, support and "back office" systems, based upon a clear understanding of the mandate requirements and

how to develop and integrate its requirements into vehicle parts and systems. V2V will be integrated with many other vehicle systems and functions, including Vehicle Networks, Cybersecurity, Telematics/Infotainment, Chassis/Body, Powertrain Control, IT, Electrical Controls/Displays, Antennas and more. As a result, Manufacturers will need more time than the proposal provides in order to deliver fully developed, validated and mandate-compliant products that compatibly communicate across manufacturers' devices to create the V2V system of safety information sharing.

We suggest two changes:
a. A longer lead time from final rule to first mandated products of at least 3 years.
b. A less aggressive four year phase-in, such as: 25%, 50%, 75%, and 100% over the course of consecutive years.

NCTA – The Internet and Television Association: The [Federal Communications Commission] has ... identified the 5.9 GHz band for sharing and has undertaken a multi-year rulemaking and testing process to discern the best sharing technology. Because dedicated short range communications (DSRC) technologies are still in the pilot phase and have not yet been widely deployed commercially, now is the time for the FCC to identify an optimized sharing approach that will allow both V2V safety messages and Wi-Fi to flourish in the band. Without careful consideration, NHTSA's regulatory mandate could undo this important endeavor and waste years of FCC and industry effort to bring high speed broadband over Wi-Fi to consumers. Unfortunately, the NPRM has not undertaken this consideration and does not reflect the costs of the proposed new regulation on national spectrum policy or on investment in and deployment of mobile broadband.

We therefore recommend that NHTSA act in this proceeding, consistent with governing law, to:
• Recognize the differing jurisdictions of NHTSA and the FCC. NHTSA lacks jurisdiction over spectrum policy and interference issues, which have been delegated by Congress to the FCC;
• Accurately account in its cost-benefit analysis for the significant opportunity cost of restricting wireless broadband associated with the proposed mandate;
• Decline to impose a mandate that companies adopt a specific technology, chosen by the agency, to achieve safety goals in light of the excessive costs of doing so; and
• Consider meaningful regulatory alternatives to such a mandate.

CISCO: In the vehicular transportation segment, Cisco has authored a reference architecture for roadside deployment of Dedicated Short Range Communications (DSRC); we have proposed a potential technology solution to allow Wi-Fi to share DSRC spectrum without harmful interference to DSRC; we are activity working with the automotive industry on in-vehicle networking; and we offer cloud services to automotive manufacturers to manage data generated by vehicular systems for the service of the existing fleet and future
design of vehicles. ...

Cisco ... agrees with the Notice's finding that DSRC is "the only mature communication option that meets the latency requirements to support vehicle communication based crash avoidance." DSRC technology, and in particular the BSM, has undergone extensive testing under the direction of the Department of Transportation (DOT), and has been deployed in a wide array of demonstration projects. Business model issues are largely settled in that there is a clear idea of the cost of adding the technology to light vehicles, and that the radio would be maintained and supported over time by the automotive OEMs similar to other safety technologies in vehicles today. Beyond the purchase price of the vehicle, consumers would not be asked to pay a subscription fee. ... A number of radio vendors offer DSRC,

including aftermarket products that can help accelerate DSRC adoption, and DSRC is now shipping as standard equipment in GM Cadillac CTS models. Use cases are proliferating, and related standards work continues to advance....

As a technology vendor, Cisco is now beginning to see evidence of state implementation of roadside DSRC systems independent of the BSM-focused demonstration projects to date. Cisco further believes that cellular-based systems have great promise to address radiobased safety communications in the future, recognizing that the application of this technology is not as mature as DSRC today. Up until recently, the standards on which 4G LTE systems are based could not reasonably address radio-based communications safety for vehicles. The deficiencies were many – failure to meet latency requirements, coverage, lack of a V2V capability, etc. That is beginning to change with industry adoption of new cellular standards for V2V, and we are beginning to see the first testing initiatives for safety applications of the new radios that are based on these standards, including radios that enable direct V2V communication without routing transmissions through infrastructure.

Industry weighs in on DSRC for V2V communications (Part 2)
RCR Wireless News
Kelly Hill
April 14, 2017

NXP claims technology leadership in DSRC rulemaking comments

As the cellular industry and standards bodies increasingly seek to support connected vehicles, the federal government is considering whether to mandate the use of Dedicated Short-Range Communications capabilities — or interoperability with DSRC — in all new light vehicles. The public comment period for the National Highway Transportation Safety Administration's proposed Federal Motor Vehicle Safety Standard (FMVSS) DSRC rulemaking closed this week.

Below are selected excerpts from telecom and transportation companies and organizations on the National Proposed Rulemaking, which would involve a timeframe in which a final rule on the subject would be made in 2019, a phase-in period would begin in 2021 and compliance would be required by 2023. (Read comments from AT&T, Verizon and others in Part One.)

NXP: NXP is the DSRC V2X technology leader with its RoadLINK solution, a complete, automotive grade, secure V2X system solution, currently in production with a major NA OEM. Security in wireless communications is paramount; and is why the RoadLINK system solution incorporates a high performance secure element comparable with the standards of banking cards or electronic passports designed to deter and prevent hacking attacks in the connected car. After more than 1 million days of V2X testing, we are contributing to the 'state of the art' and are convinced that the technology is mature, safe and ready for deployment worldwide. NXP endorses NHTSA's conclusion that short of a mandate, reaching a critical mass of vehicles with vehicle-to-vehicle communications ("V2V") capability to realize the full potential of safety benefits faces great uncertainty. NXP supports a mandate over a "if-equipped" standard to achieve a critical mass in the quickest timeframe possible.

NHTSA proposes a two-year lead-time after the final rule is adopted to begin the phase-in period. As mentioned previously, NXP's DSRC IEEE 802.11p RoadLINK solution is a complete automotive grade, secure V2X system solution, currently in production with a major NA OEM. As the V2X industry chipset leader we believe the semiconductor industry will be ready to fully support the phase-in period.The

NPRM proposes to mandate the use of IEEE 802.11p technology as the basis for V2V communications in the 5.9 GHz band. Currently a debate is on-going between supporters of DSRC IEEE 802.11p and cellular technology over the suitability of each supporter's technology for secure, reliable, and low latency V2V communication for safety applications. NXP believes that DSRC IEEE 802.11p is the only proven and production ready technology today that meets the V2V safety requirements. It is reasonable to envision that given significant time and investment, an automotive grade LTE V2V technology and product suitable for V2V safety applications could eventually be achieved and ready for mass deployment, but only after extensive testing and validation including interoperability with DSRC radios.

As NXP, we fully support the proposed mandate of DSRC technology for V2V while recognizing the potential for coexistence with an interoperable alternative such as LTE/5G technology. Yet the mandate and rollout of the lifesaving DSRC technology should not be further delayed while the cellular community continues to work on their LTE/5G V2V standards and eventual product development, testing and validation.

Qualcomm: As a strong and long-standing believer in the value of V2V safety communications, Qualcomm has been developing both the original DSRC technology and, more recently, 4G LTE-based and 5G cellular technologies (known as Cellular V2X or C-V2X) to support V2V communications. Qualcomm strongly supports the pressing need for V2V operations in dedicated licensed spectrum and integration into vehicles to improve roadway safety and save lives.

As noted in the NPRM, technological innovation in this area is ongoing and is one of Qualcomm's core foci…. We provided technical support as DSRC progressed from applied research to pilot tests, culminating in the safety pilot that validated the hypothesis that V2V communications can indeed save lives on our nation's roads. Qualcomm has continued to innovate with our automotive partners and is currently expanding the V2V safety opportunity beyond DSRC to include Cellular V2X (4G LTE-based and 5G technologies), which bring additional benefits. Qualcomm's wireless chips were in the DSRC equipment used by the Crash Avoidance Metrics Partnership ("CAMP") and DOT in Safety Pilot Driver Clinics and Model Deployment work, and our chipsets will be used in upcoming trials around the world to demonstrate the viability of using cellular direct communications connectivity for V2V safety applications. We are working with automakers to incorporate these technologies into solutions that can support any new Federal Motor Vehicle Safety Standard ("FMVSS"). …

Qualcomm asks NHTSA to consider interoperability beyond the constraining premise in the NPRM that DSRC will be first in the field and that alternative technologies would have to interoperate with DSRC equipment (e.g., by receiving BSMs). Defining interoperability in this way impedes innovation and could impede the U.S. from experiencing important mission critical benefits of the 5G future. To be clear, Qualcomm supports DSRC as a useful technology, but the NPRM's definition of interoperability picks DSRC as the de facto technology winner. We believe there should be an objective evaluation based on realistic deployment models that assess variations of a mandate and market penetration of 4G LTE and 5G devices that include C-V2X capabilities.

NGMN Alliance: NGMN recognizes that during the past ten years substantial efforts were taken to develop and test these use cases based on DSRC technology, however we would like to note that cellular-based communication technology already has been widely deployed within vehicles (and is increasing in adoption), not only for information and entertainment purposes but also for the purpose of maintaining and increasing safety and security including software updates. We note that the cellular attach rate for newly manufactured vehicles in the North America market already has line-of-sight to

achieving nearly 100% penetration. This includes a present state where automotive OEMs are effectively and increasingly leveraging cellular connectivity for updates ranging in size from 5 MB to 1 GB.

Furthermore, NGMN has already identified that some of the proposed V2V safety applications cannot be implemented effectively with DSRC technology. For instance, the DNPW application may require a higher distance range than what will be supported for DSRC BSMs (300 m), when vehicles are travelling at high speeds. As described in Chapter 5, C-V2X nearly doubles the communication range which can better address the DNPW at high speeds. It can also be expected that currently proposed and future V2X applications may be implemented with significantly higher performance standards and would allow for a better experience if using C-V2X.

In addition, today's market has shown that some safety use cases have been already implemented utilizing cellular connectivity and related backend services. Examples in this area include, forward collision warnings based on crowd sourced sensor information of location and the speed of multiple vehicles (see for example commercial services at HERE, TomTom, Inrix et al.), and hazardous location warnings emanating from a backend service based on emergency brake lights or blocked lanes indicated by crowd sourced vehicle sensor information (see e.g. Daimler, V2X series product). Those kinds of applications and their market success can be even accelerated and widened by a mandate. From the customer's perspective, the benefit of using cellular technology and backend services for safety applications in parallel to direct V2V communication may be achieved from day one, because the service is not strictly dependent on the availability of other cars as direct communication partners.

BMW: In general, BMW believes that the NPRM should be amended to be technology neutral by giving adequate consideration to all communication technologies when prescribing specific requirements and not solely focusing on Dedicated Short Range Communication (DSRC). While the regulatory text makes an attempt to leave the door open for interoperability with other communication technologies, this attempt is biased in its requirement that these other technologies must be able to communicate with DSRC, but not the other way around. DSRC is therefore effectively mandated as a standalone technology. BMW believes that many of the shortcomings of DSRC can be efficiently and cost effectively addressed by Cellular-V2X technologies in the very near future … . We urge the agency to consider rewriting the requirements of this rule to be performance-oriented and technology neutral.

Wi-Fi Alliance: Wi-Fi Alliance strongly supports NHTSA's goal of promoting vehicle safety. Pursuing that goal should proceed in parallel with the efforts of the Federal Communications Commission ("FCC") and Department of Transportation ("DoT") to determine how the 5850-5925 MHz band (the "5.9 GHz band") can be shared between the Dedicated Short-range Radio Communication ("DSRC") service – which NHTSA envisions will support V2V communications – and unlicensed devices. That work is ongoing and allowing time for a full assessment of the potential for sharing is critical to determining how the 5.9 GHz band can satisfy the needs of V2V communications and the skyrocketing demand for unlicensed spectrum capacity. … NHTSA should remain conscious of the integral part that Wi-Fi plays in the communications ecosystem and that the FCC, with DoT's input, is evaluating the potential shared use of the 5.9 GHz band by Wi-Fi and DSRC systems.

National Transportation Safety Board: During recent NTSB crash investigations, we determined that collision warning and avoidance systems capable of storing and retrieving vehicle and system performance information would aid in the evaluation and improvement of such systems, as well as facilitate a better understanding of crashes. For example, we recently investigated a multivehicle crash in Cranbury, New Jersey, in which a truck-tractor semitrailer failed to slow for stopped traffic in an active

work zone and struck a limo van. Twenty-one people in six vehicles were involved in the crash. One limo van passenger died, and four other passengers were seriously injured. The truck-tractor was equipped with an advanced braking system capable of providing FCW alerts to the fatigued driver. However, because of limited data recording capability, the system did not record any forward radar sensor data, which made it difficult to analyze and assess both the crash and the system's performance. As a result of this investigation, the NTSB recommended that manufacturers of collision warning and avoidance systems for use on commercial vehicles include in those systems the capability to store and retrieve data pertaining to object detection, driver audible/visual alerts, and interventions for a period and at a data rate adequate to support crash investigation and reconstruction. ... The NTSB maintains that NHTSA should consider developing minimum data recording requirements for V2V technology to ensure a crash-hardened system with a minimum retention period and data rate adequate to analyze system performance and make necessary improvements.

Cable Clashes With DOT Over Spectrum
Light Reading
Mari Sibley
April 13, 2017

In the cable industry's unending quest for unlicensed wireless spectrum, the NCTA has run up against the US Department of Transportation's own spectrum quest.

The National Cable & Telecommunications Association (NCTA) filed last-minute comments yesterday on a proposal by the DOT to mandate Dedicated Short Range Communications technology in vehicles for vehicle-to-vehicle communications. The DOT believes DSRC could radically improve road safety by allowing cars to communicate with each other using Basic Safety Messages (BSM) that share information about a vehicle's speed, direction, momentum and more. However, the NCTA has concerns about the spectrum being used to support these V2V communications; namely, how much real estate in the 5.9GHz frequency band any mandated V2V technology could section off from other applications.

According to the NCTA, "the 5.9 GHz band is widely recognized as the single best hope to address the current Wi-Fi spectrum deficit." As such, the NCTA doesn't want the DOT to make rules on how the spectrum is used until studies have been completed on how best to manage spectrum-sharing in the frequency band to meet all needs.

Currently, the Federal Communications Commission (FCC) is studying two proposed spectrum-sharing approaches. The first, called "detect and avoid" or "detect and vacate," would prevent unlicensed devices from using the entire DSRC spectrum band if any DSRC signals were detected. The second, called "re-channelization," would break up the spectrum band into two blocks, maintaining one for safety-related communications that would then be unavailable for unlicensed devices.

The NCTA sees potential problems with both strategies. The cable trade association notes that the "some have advocated before the FCC that the detect-and-vacate approach to coexistence would render the entire 5.9 GHz band unusable for Wi-Fi," and could cost the industry between $10 and $20 billion per year in lost use. The NCTA adds that the re-channelization approach would cause less financial harm, but would still limit other WiFi uses of the 5.9GHz band.
In its comments, the NCTA urges several actions by the DOT and its subsidiary, the National Highway Traffic Safety Administration (NHTSA). The NCTA recommends that the NHTSA do a better job in conducting its cost-benefit analysis by taking into account lost WiFi opportunities. And it recommends

that the NHTSA not mandate a specific technology for achieving safety goals given the costs involved. The NCTA also notes that the NHTSA should leave spectrum policy issues to the FCC, which has the jurisdiction to govern on them.

If there's one thing the contretemps between the NCTA and the DOT highlights, it's how debate over spectrum use will continue to extend into new areas as more and more devices need wireless frequency access to connect and communicate. Considering all of the smart-city applications that have yet to be implemented, it's a guarantee that spectrum fights will only grow more contentious moving forward.

Meanwhile, the cable industry isn't going to back off in fighting for access to more unlicensed spectrum given that it relies on that connectivity for wireless services. Aside from MVNO agreements with Verizon Communications Inc.(NYSE: VZ), and the possibility that Comcast Corp. (Nasdaq: CMCSA, CMCSK) could acquire spectrum in the 600MHz auction, WiFi is pretty much all that cable's got. (See New Comcast Wireless Details Drop This Week .)

NCTA: V2V Proposal Is Straying Into FCC's Lane
Broadcasting & Cable
John Eggerton
April 12, 2017

NCTA-The Internet & Television Association has told the National Highway Traffic Safety Administration (NHTSA) that its proposal on vehicle-to-vehicle communications in the upper 5 GHz band, particularly a mandate on safety technology, is misguided and threatens the future of wireless communications.

That came in comments on an NHTSA Notice of Proposed Rulemaking.

Broadband providers have been pushing the FCC to open up the band for unlicensed wireless use--for Wi-Fi hotspots--sharing that spectrum with V2V communications, and signaled to NHTSA that it was straying into that agencies lane.

NCTA wants NHTSA to "(1) amend its cost-benefit analysis to properly account for the costs its mandate would impose on broadband consumers and investors; and (2) consider how it can advance vehicle safety while supporting the Federal Communications Commission's (FCC) efforts to permit efficient, shared use of the 5.9 GHz band."

NCTA offered up some statistics to bolster its case, including hundreds of millions of dollars in investment to deploy Wi-Fi networks; 2.5 billion active Wi-Fi sessions daily, 169 petabytes of data, predictions of the U.S. needing 1.6 GHz of new Wi-Fi spectrum by 2025.

The Department of Transportation (of which NHTSA is a part) issued the NPRM back in December, mandating V2V communications (using dedicated short-range communications, or DSRC) on all passenger cars and trucks, which it said would prevent hundreds of thousands of crashes. It would also "require that all V2V devices must 'speak the same language' through a standard technology.

NCTA says NHTSA's proposal does not accurately account for the opportunity cost of the mandate and asked it not to impose a mandate "that companies adopt a specific technology, chosen by the agency, to achieve safety goals in light of the excessive costs of doing so."

It also said NHTSA does not have the authority to mandate that all basic safety messages (BSM) be transmitted on a specific channel, which is under FCC authority.

NCTA also wants NHTSA to defer to the FCC when it comes to vetting proposals on how V2V and the Wi-Fi the hot spots that have been ISPs primary mobile broadband play can share the spectrum, saying "this, too falls within the FCC's authority [and expertise] not NHTSA's."
NCTA says NHTSA is straying into spectrum policy, over which it has no authority.

"Unfortunately, after recognizing NHTSA's limited jurisdiction, the NPRM improperly expands NHTSA's regulatory reach into areas that Congress assigned to the FCC," it said. "If NHTSA moves forward with the proposed mandate, it can establish safety standards for V2V technology, consistent with its jurisdictional limitations. But it must do so without deciding questions of spectrum policy that fall outside its jurisdiction—directly or indirectly. NHTSA must address these fundamental problems before moving forward with a V2V rule and must defer to the FCC's authority and expertise in spectrum management."

"We are reiterating our concerns about NHTSA's DSRC mandate for all new cars in this filing," said John Gasparini, policy fellow at Public Knowledge. "In recent months, we've seen a dramatic increase in consumer interest in privacy and cybersecurity protections. While consumers clamor for greater protections, however, NHTSA continues advancing a proposal that would mandate a vehicular technology that not only lacks adequate privacy or cybersecurity protections but also remains open to commercial use."

Former DHS official says connected-car network needs cybersecurity framework
Inside Cybersecurity
Joshua Higgins
April 4, 2017

The network supporting connected vehicles needs a cybersecurity framework or standard along with a compliance regime for auto manufacturers, according to a former Department of Homeland Security official and National Institute of Standards and Technology researcher.

Alex Kreilein, co-founder and managing partner of SecureSet, writes in a new report that the emerging dedicated short-range communications system, or DSRC, which underpins vehicle-to-vehicle and vehicle-to-infrastructure communications, is vulnerable to cyber threats and therefore additional cybersecurity controls should be put in place.

Kreilein served as a lead technology and cybersecurity strategist at DHS from 2011-2015 and was a guest researcher at NIST.

"Given the demonstrable vulnerabilities in modern and connected vehicles, mitigations must be developed to address risks to life and safety…" the report states. "In this way, the automotive community can continue its legacy of safety engineering, which consumers have come to expect due to decades of diligent work by vehicle manufacturers. Vehicle security architectures are necessary to protect consumers, to protect the investment in DSRC, and to protect the future of automotive innovation."

The National Highway Traffic Safety Administration has been moving forward with a rulemaking requiring automakers to include DSRC devices in their products in order to establish the V2V system, which is touted as a life-saving safety feature for new automobiles. Through that effort, NHTSA has set up an effort to create a "security credential management system" for DSRC that mitigates security risks.

Kreilein filed the report to NHTSA in response to the administration's efforts to gather feedback on its rulemaking process. NHTSA has been soliciting comments on safety standards mandating automakers to implement DSRC communications devices in their products. The administration is seeking comments through April 12, when it will then review the comments received and move forward with its rulemaking.

The report says the security credential management system "shows real value," but implementing the proposal in a practical matter remains to be seen.

"In any event, it remains only a proof-of-concept, and will likely not be 'production ready' for some time even though it appears that NHTSA is ready to 'green light' the use of DSRC," the report states.

An industry source told Inside Cybersecurity that the security management system would be difficult to scale across the American automotive fleet.

But the Kreilein report warns that if cybersecurity is not addressed beforehand, DSRC could pose a significant cyber threat to automobiles.

"Empirical security research already shows the general lack of security in vehicles," the report states. "DSRC, as presently conceived, would make matters worse. It presents a new attack surface with special considerations, given its integration into critical control systems. The absence of security frameworks or a compliance regime risks life and safety."

To address this, Kreilein writes that the industry should establish compliance with a "reasonable" security framework.

"Without a framework, the ills of the broader IT market will be realized in vehicles, privacy and security will be risked and the costs of security will not be easily controlled, disproportionately harming those with the least amount of economic agency," Kreilein writes. "It is necessary for the industry to ensure that the use of DSRC is predicated on the compliance with a reasonable security framework, which it currently lacks. This approach supports both motorists and automotive [original equipment manufacturers]."

The security of NHTSA's DSRC proposal has come under scrutiny before, as privacy advocates and other groups have urged the Federal Communications Commission to step in to require cybersecurity and privacy strategies before DSRC devices are deployed.

The FCC under the Obama administration declined to take direct action, rather saying they would work with NHSTA and other agencies to assure connected cars are adequately secured.

Securing our intelligent, interconnected vehicles
Tech Writers Bureau
William Jackson

March 31, 2017

The Dedicated Short Range Communications (DSRC) standard is being developed to meet the emerging needs of our increasingly interconnected transportation systems. The Federal Communications Commission has dedicated spectrum for Intelligent Transportation Systems, and the Transportation Department is spearheading development of DSRC to support operational communications among vehicles and with the transportation infrastructure.

But one researcher warns that more thought must be given to security before the standard is widely deployed in our automobiles and trucks, and is calling for development an industry security framework.

“Empirical security research already shows the general lack of security in vehicles,” Alex Kreilein, a managing partner of the security services firm SecureSet, writes. “DSRC, as presently conceived, would make matters worse. The absence of security frameworks or a compliance regime risks life and safety.”

The problem is not that DSRC is bad. The problem is the assumptions that it will work as intended, that software and hardware implementations will be error-free, and that it will not be attacked. “The notion that DSRC will be vulnerability free is fanciful at best,” Kreilein writes. “Without a robust security architecture, DSRC will inevitably fall victim to intrusion by a malicious party.”

The threat is multiplied by the creation of a communications monoculture that could make many vehicles and systems vulnerable to a single exploit.

There is a great need for a secure communications standard for autos. Modern cars already contain hundreds of Electronic Control Units, which gather and transmit data for critical systems such as breaking and steering as well as for on-board infotainment systems. They use Controller Area Networks to communicate. These systems will increasingly be communicating with other vehicles and outside infrastructure, and playing a greater role in actually controlling vehicles. Reliability and security are essential to prevent a crash—both of computers and of vehicles.

Current security requirements for DSRC focus on cryptography, which Kreilein says is a necessary by insufficient element. “It lacks mitigations for the well documented tactics, techniques, and procedures used by attackers. The current standard lacks the common concept of defense-in-depth.” Automotive equipment manufacturers that produce the hundreds of components comprising both critical and non-critical systems need a common security architecture that separates and protects both critical and non-critical segments.

Kreilein proposes a system of self-regulation much like the Payment Card Industry Data Security Standards that would include binding contracts that could be enforced by the Federal Trade Commission. The standards would not have to be created from scratch; Kreilein notes that researchers already have tackled many of the challenges of developing security frameworks, but that the work has not been integrated into DSRC.

Existing vulnerabilities in automotive electronics and recent experiences with hackers turning the embedded technology of the Internet of Things against us demonstrate the necessity of building security into our smart, interconnected and increasingly automated transportation systems. The integration of networked electronics into our vehicles is already under way, but we are still early enough in the process that there is time to standardize on a secure platform.

Kreilein points out that DSRC is only one of the attack surfaces in modern vehicles and that protecting it will not guarantee overall security. But it is essential that our vehicles' communications protocols be secure. Whether this proposal is the best way to do it is open to debate, but it is an issue that should be addressed as early as possible to ensure the safety and reliability of our next generation of automobiles.

Cyber Issues Must Be Addressed Before DSRC is Launched, Report Says
TR Daily
Paul Kirby
March 30, 2017

Before dedicated short-range communications (DSRC) networks are launched, cybersecurity must be addressed, according to a paper submitted to the National Highway Traffic Safety Administration today in response to a notice of proposed rulemaking released in December proposing to require that all new light vehicles have vehicle-to-vehicle (V2V) technology to help drivers avoid crashes (TRDaily, Dec. 13, 2016).

"Empirical security research already shows the general lack of security in vehicles," said the paper. "DSRC, as presently conceived, would make matters worse. It presents a new attack surface with special considerations, given its integration into critical control systems. The absence of security frameworks or a compliance regime risks life and safety. Providing a basic standard of care cannot be left to the market for safety-of-life systems—it is not in the case of PCI DSS, HIPPA, and a number of other standards. Without a framework, the ills of the broader IT market will be realized in vehicles, privacy and security will be risked, and the costs of security will not be easily controlled, disproportionately harming those with the least amount of economic agency.

"It is necessary for the industry to ensure that the use of DSRC is predicated on the compliance with a reasonable security framework, which it currently lacks," the paper added. "This approach supports both motorists and automotive OEMs."

The paper was written by Alex Kreilein, cofounder and managing partner of SecureSet.

Last year, Public Knowledge and the New America Foundation's Open Technology Institute filed a petition with the FCC for an emergency stay and rulemaking asking the agency to develop DSRC rules that protect the cybersecurity and privacy of connected-vehicle users.

Full Text - Op-Ed, Blog Posts, and Third Party Statements

Straight Talk on the "Talking Car" Mandate
Real Clear Future
Marc Scribner
May 24, 2017

Will another driver's car "talking" with yours someday save your life? The answer, from regulators and many automakers, is a resounding "Yes." Such a promising technology should have many takers. So why are federal regulators seeking to force it on the public?

To that end, the National Highway Traffic Safety Administration (NHTSA) in the final days of the Obama administration proposed a new regulation that would mandate all new light vehicles to be installed with technology to enable vehicle-to-vehicle (V2V) communications. The proposal aims to require cars to connect to one another at a distance of up to 300 meters, to allow the transmission of direction, speed, and braking information that could alert drivers to approaching hazards, such as stalled vehicles and drivers running red lights. NHTSA estimates that by 2060, for a cost of up to $109 billion—the second-most expensive car regulation this decade—the mandated technology could save between 987 and 1,365 lives annually.

That is the narrative advanced by proponents of a forced V2V regulation. Unfortunately, it ignores key challenges facing widespread deployment—and thereby any consumer benefits. The proposal relies heavily on an obsolete communications protocol, to the detriment of superior competing technologies. This protocol, called dedicated short-range communications (DSRC), has enjoyed exclusive use of certain airwaves allocated by the Federal Communications Commission in 1999.

This largely unused block of radio spectrum sits immediately adjacent to the frequencies used by Wi-Fi devices, which face growing congestion problems. The cable and wireless industries have been lobbying to gain access to this spectrum block, arguing that current policy has resulted in billions of dollars in lost economic opportunity. Indeed, one study estimates that allowing Wi-Fi devices to share this spectrum would result in benefits to the economy between $191 and $744 billion dollars.

NHTSA also envisions the installation of nearly 20,000 roadside equipment units across the nation's highways. The agency concedes it does not yet know who would operate this new infrastructure network, let alone how it will be funded and maintained. Yet, the answer to safer roadways is in plain sight.

The private sector has been working on V2V technologies to harness existing cellular networks, an approach that would address the operations, funding, and maintenance issues that have stumped the government for years. A number of these innovations are already standard in cars on the road today.

If that weren't enough to wave the government away from an unnecessary, burdensome regulation: privacy and cybersecurity concerns loom large in this proposed rule, given the importance of maintaining safety data integrity. NHTSA proposes encrypting messages with digital certificates to limit misuse, but the agency was unable to develop any regulatory text, leaving a glaring, bracketed gap in the proposed rule. The public and outside experts deserve the opportunity to evaluate this critical element.

NHTSA, recognizing its legal limitations and expected public anxiety over privacy and cybersecurity, suggests that any wireless update of V2V software or supply of additional digital certificates should require owner consent. The agency opposes allowing consumers to opt out of V2V, but requiring consent prior to updates provides consumers a backdoor opt-out. If an owner refuses a critical software update or fails to replenish digital certificates, the DSRC-run V2V device becomes inoperative. But this technology only works if it's widely deployed, a Catch-22 in this scenario.

NHTSA proposes to mitigate this problem by requiring that telltale lamps or dashboard messages prod owners to accept updates. But given that nearly 10 percent of vehicles on the road today display a "check engine" light and the expected public objections to mandated V2V, NHTSA ought to consider how "apathy rates" as well as "misuse rates" could affect deployment.

And several automakers want NHTSA to pump the brakes. Tesla Motors has warned the agency that "the implementation of V2V communications will exponentially increase the cybersecurity attack surface of a vehicle's interrelated systems" and that the rise of onboard sensors to enable autonomous driving "will outpace the rulemaking trajectory of V2V communications." Thus, the company "questions the need for this rulemaking." Mercedes also weighed in with similar cautions.

Federal regulators and traditional automakers have invested considerable time and resources into V2V. Vehicle connectivity itself is not the problem. But the technology contemplated in the proposed mandate will be a decade out of date by the time the phase-in begins and two decades obsolete at the projected cost-benefit break-even point, around 2030.

The uncomfortable truth is that early V2V adopters can expect to enjoy nonexistent to trivial safety benefits, as V2V only provides benefits when a significant percentage of the nation's auto fleet is equipped with the technology. It is projected to take decades before adoption reaches a level where drivers have greater than a coin-flip's chance of V2V preventing a crash.

In contrast, vehicles with automated systems along the lines of those being developed by numerous private firms—from automatic emergency braking and lane-keeping to full self-driving vehicles—can deliver immediate benefits to consumers and the long-term safety potential is far greater than that of V2V hazard warnings.

Rather than mandate V2V, or any other technology, federal regulators should adopt a hands-off approach to the rapidly evolving auto technology landscape. Allowing the private sector to continue to develop innovative ways to improve auto safety is the best way to prevent crashes and save lives.

Danger Ahead: The Government's Plan for Vehicle-to-Vehicle Communication Threatens Privacy, Security, and Common Sense
EFF
Jamie Williams
May 8, 2017

Imagine if your car could send messages about its speed and movements to other cars on the road around it. That's the dream of the National Highway Traffic Safety Administration (NHTSA), which thinks of Vehicle-to-Vehicle (V2V) communication technology as the leading solution for reducing accident rates in the United States. But there's a huge problem: it's extremely difficult to have cars "talk" to each other in a way that protects the privacy and security of the people inside them, and NHTSA's proposal doesn't come close to successfully addressing those issues. EFF filed public comments with both NHTSA

and the FTC explaining why it needs to go back to the drawing board—and spend some serious time there—before moving forward with any V2V proposal.

NHTSA's Plan

NHTSA's V2V plan involves installing special devices in cars that will broadcast and receive Basic Safety Messages (BSMs) via short-range wireless communication channels. These messages will include information about a vehicle's speed, brake status, etc. But one big problem is that by broadcasting unencrypted data about themselves at all times, cars with these devices will be incredibly easy to track. All you would need is a device that could intercept these messages. NHTSA is aware of this huge privacy problem and tried to develop a plan to make it harder to link V2V transmissions with particular vehicles, while still including enough information for the receiver to be able to trust a message's content. But NHTSA's plan—which involves giving each car 20 rotating cryptographic certificates per week to be distributed and managed by a complicated public key infrastructure (PKI)—didn't achieve either objective.

The Problems

One of the fundamental problems with NHTSA's plan is that assigning each vehicle a mere 20 identities over the coarse of an entire week will do the opposite of protecting privacy; it will give anyone who wishes to track cars a straightforward way to do so. NHTSA proposes that a car's certificate change every five minutes, rotating through the complete batch of 20 certificates once every 100 minutes. The car would get a new batch of 20 certificates the next week. As we explained in our comments, while a human being might find it confusing or burdensome to remember 20 different identities for the same vehicle, a computer could easily analyze data collected via a sensor network to identify a vehicle over the course of one day. It would then be able to identify and track the vehicle for the rest of the week via its known certificates. The sensor network would have to complete this same process every week, for every new batch of certificates, but given how simple the process would be, this wouldn't present a true barrier to a person or organization seeking to track vehicles. And because human mobility patterns are "highly unique," it would be easy—in the case of a vehicle used in its ordinary way—to recognize and track a vehicle from week to week, even as the vehicle's list of 20 assigned certificates changed.

NHTSA seems to presume that no one will make long-term, systematic efforts to track vehicles. But this presumption is incredibly naïve. We have learned the hard way that both the government and private companies will go to great lengths to track vehicles—just look at the proliferation of Automated License Plate Readers (ALPR). V2V will make these tracking efforts easier, by making it significantly cheaper to get more reliable information about a vehicle's whereabouts, more of the time, in more situations, in a clandestine manner, without requiring a line-of-sight to a vehicle's license plate.

There are other fundamental problems with NHTSA's plan. First, NHTSA proposes the creation of a new public key infrastructure (PKI) to solve a problem that PKIs simply cannot—and were never intended—to solve, demonstrating a serious misunderstanding of the technology. The sole purpose of a distributed PKI system is to determine who or what produced a validly signed message. A PKI system, for example, cannot establish that the content of the message is "safe" and truthful and therefore the reliable basis for decisions. But NHTSA's plan suggests that use of a PKI would enable vehicles to assess whether messages it receives are "safe" in this way. This will create widespread—and potentially quite dangerous—confusion about the level of confidence that should be placed in the contents of a validly signed message. NHTSA's failure to understand the inherent limits of PKIs is deeply troubling.

Second, NHTSA's envisioned PKI is much larger and more complicated than anything in existence, yet it fails to account for known—and considerable—technical challenges presented by smaller systems. For instance, in the WebPKI—used to distribute and manage HTTPS certificates for websites—it has proven extraordinarily difficult to phase out cryptographic algorithms after they are discovered to be insecure. It took four years, for instance, to phase out (or deprecate) the hash algorithm SHA-1. NHTSA proposes a more complicated PKI, which would issue orders of magnitude more certificates, without even attempting to address the fundamental functional challenges that we already know exist.

Third, NHTSA's plan for dealing with "bad actors" is to revoke their certificate and push out certificate revocation lists (CRLs) to all vehicles participating in the system. But this just won't work. Not only will after-the-fact revocation be too late to prevent the first—and potentially catastrophic—attack, but sending out CLRs to every single vehicle participating in the system would take a tremendous amount of data. CRL distribution in the WebPKI has received widespread criticism for being extremely traffic-intensive and inefficient, and the CRLs NHTSA envisions would be orders of magnitude larger than the largest CRLs used in the WebPKI—we're talking gigabytes of data being distributed to each car in the United States on a regular basis.

What's more, the plan opens cars up to an entirely new surface of attack while failing to address serious security concerns, putting people at risk of potentially grave harm.

And the plan makes absolutely no sense from a cost-benefit perspective. Because V2V only works when lots of cars have the devices, it will take a great deal of time and money—$33 billion to $75 billion over the course of 15 years—before there is any payoff in terms of increased safety. And by that time, given the exponential rate of technological development in mobile data networks alone, it's likely the technology will be obsolete. Automobile manufacturers have come out in support of the proposal, arguing that over $1 billion has already been invested in V2V. But that's not a reason to keep moving ahead with a flawed idea, especially when so much more will need to be spent. As laid out in detail by Brad Templeton, Chairman Emeritus of EFF's Board and a developer of and commentator on self-driving cars, "[V2V's] cost is high, and those resources could be much better spent." For this reason alone, NHTSA needs to move on from its outdated and backwards looking proposal.

We've made sure both NHTSA and the FTC heard our concerns loud and clear. Since submitting comments to the FTC, we've been invited to participate in a workshop in June dedicated to examining the privacy and security issues posed by connected vehicles. Senior Staff Technologist and former autonomous vehicle researcher Jeremy Gillula will be there to explain why the FTC should put the brakes on NHTSA's misguided and potentially disastrous plan.

EFF is not alone in our concern over NHTSA's V2V plan. Many other organizations have filed comments expressing their own concerns with the troubling proposal. We hope NHTSA heeds these warnings—for the good of all of us.

Senseless Government Rules Could Cripple the Robo-Car Revolution
Wired
Ryan Hagemann
May 1, 2017

FEW TECHNOLOGICAL ADVANCEMENTS bring to mind the American spirit of innovation like Henry Ford and his Model T. In the wake of his transportation innovation, the horse and buggy became an anachronism as the mass-produced automobile reshaped our cities, led to the emergence (for better or worse) of the suburbs, and revolutionized how we move goods and people.

Now, there's little doubt that autonomous vehicles are the next frontier of transportation. These vehicles are projected to make our roads safer, potentially reducing fatalities by orders of magnitude. Along the way, however, there are a number of roadblocks to surmount: infrastructure issues, restrictive state licensing policies, driver education, cybersecurity and privacy vulnerabilities, and more. For innovators, regulators, and policymakers, solving these problems will involve a long to-do list, but a pointless regulatory scuffle over technology standards should not be on it.

So why is the federal agency responsible for our road safety looking to introduce a totally avoidable roadblock to automotive innovation by mandating a severely flawed technological standard for vehicle communications?

Here's the debate: Autonomous vehicles of the future will need to communicate with each other and the infrastructure around them, signaling to avoid collisions and informing other cars about traffic and road conditions. Cars will need to sense pedestrians and wildlife, and generally become better drivers than we are. There are two leading contenders for how this communication will happen: Dedicated Short Range Communications (DSRC) and next-generation wireless 5G networks.

Some auto manufacturers have already placed their bets: The 2017 Cadillac CTS sedan rolled out with DSRC technology earlier this year, right around the time Volkswagen announced all of its autonomous vehicles will be powered by 5G. Sensors like light image detecting and radar (LIDAR), cameras, and GPS-based technologies already help cars automatically brake, keep vehicles in the proper lanes, and warn drivers of impending obstructions. Here, safety and innovation are complementary concepts.

The National Highway Traffic Safety Administration (NHTSA) is in the process of carrying out a 2016 mandate for vehicle-to-vehicle (V2V) communication standards. Supporting V2V communications standards is a laudable goal. But the technology should be developed through a competitive market-oriented process, not imposed by government regulators.

Unfortunately, NHTSA has already made a choice on behalf of innovators: DSRC. At best, this is a waste of time, money, and government resources. At worst, this is a decision that could chill a generation of vehicular innovation and safety.

Imagine if the government had demanded that Henry Ford equip every one of his Model Ts with telegraph machines that could only communicate with other Model Ts. A 19th century communications technology mandated for use in a 20th century innovation would have been a crushing blow to innovation and competition in the emerging automobile industry. That's precisely what is happening with the DSRC mandate, and the same potential for future innovation is at risk with its implementation.

Technology mandates almost never make sense. In this case, it's almost impossible to understand what NHTSA could be thinking.

Unlike other technologies we use today, a DSRC unit is useless in preventing a collision unless the other vehicle involved in the collision is also equipped with a DSRC unit. So drivers of the new, DSRC-enabled Cadillac will surely avoid other 2017 Cadillac CTS sedans, but not much else. And the technology must be available in a critical mass of cars to be beneficial for consumers. Some guessed that initial deployment of DSRC would be underway by 2006. That was seven years after the Clinton Administration's Federal Communications Commission gave automakers exclusive license to the necessary spectrum.

But here we are, nearly two decades later, and still nothing. As if that wasn't bad enough, a 2015 pilot deployment report from the Department of Transportation identified numerous failings of DSRC, from "device and interoperability issues" to cost overruns and delays.

What's more: The annual price tag of a DSRC mandate is estimated at upwards of $5 billion even after the many decades full implementation will take, and between $0.3 billion and $6.4 billion annually until then. This is the second-most expensive car-related regulation in over a decade after the most recent CAFE standards. That means consumers will pay more for cars but won't reap any of the benefits until the technology is implemented at a massive scale, which could take 20 to 30 years.

As if that all wasn't bad enough, DSRC has serious unresolved cybersecurity risks, which make a mandate to use this technology irresponsible, if not outright dangerous. Cybersecurity expert Alex Kreilein recently noted the standard's "weak privacy protections" and a susceptibility to "spread malware" in a report and filing to NHTSA.

NHTSA is considering shackling the future of driving to the success of a shaky, outdated technology that even some cellular companies have argued against.

The government shouldn't be picking which V2V standard will dominate the next few decades, especially one wracked by so many shortcomings. The last two decades of inaction on DSRC—and the vibrant ecosystem of car safety technology that has developed in the vacuum—show us that regulators cannot decide the future of car travel. This could lock up innovation and technological progress on American roadways for decades to come.

Agency resources are only getting more scarce. And truly, those resources—time, energy, and labor—should be redirected to better uses. The government should steer clear and let the innovators, not the bureaucrats, lead. The DSRC mandate should be left in the dustbin.

Otherwise, innovation and technological progress might end up in its place.

5GAA Submitted Comments to the National Highway Traffic Safety Administration
Yahoo Finance (from PR Newswire)
April 18, 2017

The 5G Automotive Association (5GAA) submitted comments to the National Highway Traffic Safety Administration (NHTSA) notice of proposed rulemaking (NPRM), "Federal Motor Vehicle Safety Standards; V2V Communications." The proposed rule is to mandate new light-duty vehicles to be equipped with dedicated short range communications (DSRC).

5GAA is a new global cross-industry association of automotive, technology and telecommunications companies and includes 42 members, of which 8 are founding members (AUDI AG, BMW Group, Daimler

AG, Ericsson, Huawei, Intel, Nokia, Qualcomm). Our mission is to enable communications solutions that address society's connected mobility and road safety needs.

In our submission , 5GAA applauds the concept behind the rule, as V2V safety is important to our technology deployment mission. 5GAA urges NHTSA to not consider just the best technology of today, but also to consider the best technologies of tomorrow. Such an approach will promote innovation and competitive market-based outcomes, ensuring that American drivers and passengers benefit from the best and most advanced safety solutions available as technology evolves. Rigid technology mandates such as specifying DSRC, whether direct or de facto, freeze technology solutions to a past point in time. NS will significantly impede the innovation and evolution path for Vehicle-to-Vehicle (V2V) safety, and positions the US to lag behind the rest of the world in V2V communications specifically as well as V2X broadly. 5GAA elaborates on the following points:

Similar to DSRC, Cellular-V2X technology for V2V safety can transmit BSM in an ad hoc manner without cellular network coverage.

Cellular-V2X technology for V2V safety communications can operate without a SIM card and offers the tools to adopt, evolve or innovate any privacy-preserving security management system including SCRM.

Cellular-V2X technology for V2V safety benefits from a significantly larger link budget than DSRC (e.g., 8 dB at high speeds), corresponding to twice the range of DSRC and higher reliability.

Cellular-V2X technology for V2V safety can support up to 50 messages per second with less than 20 msec latency.

Cellular-V2X enables V2V, and for that matter Vehicle-to-Infrastructure (V2I), Vehicle-to-Pedestrian (V2P) and Vehicle-to-Network (V2N), safety applications to take advantage of the widespread cellular network coverage in the US.

5GAA notes also that the impending launch of 5G will only widen the performance gap between Cellular-V2X and DSRC.

5GAA believes that Rather than moving forward with the proposed regulation, NHTSA should instead undertake an updated, comprehensive technology neutral analysis of V2V solutions, including DSRC and Cellular-V2X, against the performance requirements in the NPRM. If this review indicates that regulatory action is necessary, the U.S. Department of Transportation should move forward with a technology neutral regulation that sets forth minimum V2V safety performance requirements only.

The Department of Transportation's Proposed Vehicle-to-Vehicle Technology Mandate Is Unprecedented and Hasty
Mercatus Center Blog
Brent Skorup
April 14, 2017

"Connected cars" that use mobile connections to transmit and receive wireless data is a growing market. American automakers offered emergency services like OnStar for years and in recent years added wireless infotainment connections like 4G LTE and WiFi access. The next era in connected cars could be vehicle-to-vehicle (V2V) and vehicle-to-infrastructure technologies. V2V may someday alert drivers to

potential collisions that are not visible to existing sensor-based technologies. In December 2016 the National Highway Traffic Safety Administration (NHTSA) proposed to mandate a particular V2V technology standard—dedicated short-range communications (DSRC)—for all new light vehicles. NHTSA, an agency within the US Department of Transportation (DOT), boasts that this is "the first proposed mandate of V2V technology worldwide." Mandating an experimental technology like DSRC V2V is premature. The technology has not been proven economic or safe, and there should be no device mandate for light vehicles at this time.

While foresight is admirable, a device mandate for a wireless technology still in development is unprecedented. Connected cars are "just another mobile device" and would benefit from the competitive pressures seen in other mobile device markets. The Federal Communications Commission (FCC), the nation's primary wireless device regulator, generally avoids stringent device mandates because top-down control locks in technology long beyond its usefulness. Crucially, the FCC allows mobile device companies to develop their own standards and interoperability requirements.

The DOT acknowledges that "estimating the potential costs and benefits of V2V [is] quite difficult" because V2V "improve[s] safety only indirectly." The indirect safety benefits, plus the long timeline before net benefits arise, plus the unreasonably optimistic predictions of market-ready units should counsel caution. The agency's estimate that cumulative benefits will match cumulative costs in 2030 should be viewed skeptically.

At this early stage in V2V development, it is unclear whether DSRC will ever be a safe technology or whether V2V is the best way to improve auto safety. There is a significant likelihood that DSRC will be eclipsed by competing technologies, like lidar, radar, and cameras. Cellular technology may displace DSRC as a V2V technology. As ITS America has said about a parallel FCC proceeding, there is "significant regulatory uncertainty that is threatening to derail the progress that DSRC is making toward nationwide deployment."

Given the various regulatory uncertainties and DSRC's technical drawbacks, it is far too early to mandate this technology for light vehicles. In this comment, I first describe DSRC's government-directed development and slow progress. I then raise the strong possibility that other technologies will prove superior to DSRC if the market is permitted to develop, and I go on to describe DSRC's severe reliability problems. Finally, I point out that firms can develop device interoperability without an interoperability mandate.

DSRC V2V Technology Is Rigidly Prescribed and Updates Will Be Slow and Costly

It's concerning to hear that NHTSA is considering prescriptive technology mandates in the fast-moving area of connected car technology. Innovation at the speed of government, it turns out, isn't very speedy at all. Congress created the intelligent transportation system (ITS) program, which is administered by the DOT, in 1991. V2V communications is the first step towards a national ITS. The DOT has not wavered from its commitment in the 1990s to develop ITS infrastructure via "a top-down, systematic process" where, the Department says, "each component of the system" is prescribed by regulators. The notice of proposed rulemaking (NPRM) uses the language of markets, and it states that the mandate permits a "market-based approach to application development." A closer analysis reveals, however, a very limited ability to innovate upon the DSRC platform.

DSRC is a government-designed technology from top to bottom, which injects paralyzing rigidity into the system. The Federal Highway Administration considered putting DSRC in the 5.9 GHz band starting about 1996. After public consultation, the FCC set aside 75 MHz of radio spectrum in the 5.9 GHz band for ITS uses in 1999 based on a scant 19 comments and reply comments from outside parties. In 1999 and 2004, the FCC codified DSRC transmission standards, transmit power, emission mask requirements, priority framework, antenna height, and equipment certification procedures. For DSRC V2V devices, the FCC and NHTSA have prescribed or have proposed to prescribeaccess technology (IEEE 802.11p), spectrum channels (10 MHz), spectrum bands (5.9 GHz), throughput (6 Mbps), and communications technology (DSRC).

Even the DSRC device makers were hand-selected by DOT officials and subsidized.

The need to comply with the requirements from two federal agencies and satisfy multiple private and public organizations has contributed to DSRC's slow progress. The DOT started testing road safety technologies around 2000. Nevertheless, only a few firms created DSRC prototypes, and these tended to be small firms. Before 2014, there was still little improvement, little commercial interest in DSRC devices, and the DOT "took a lead role in the device development process."

Contrast the slow progress of DSRC with cellular standards. The FCC codified DSRC standards over a decade ago, and DSRC—still in the experimental phase—seems destined for the stasis associated with other FCC-mandated technology standards, like broadcast TV, which lasted largely unchanged for over 60 years. Cellular standards, on the other hand, the FCC leaves to market actors. Cellular standards have improved significantly since 2000 and have substantial market penetration, despite a lack of device mandates.

In the broader mobile communications market, access technology (WiMax, 4G LTE), spectrum channels (5 MHz pairs, 20 MHz pairs), spectrum bands (700 MHz, 1800 MHz) and communications technology (CDMA2000 1xRTT, VoLTE) change regularly in response to consumer demands, industry standards, and input availability and prices.

The competitive churn and consumer benefits are noticeable. Around 1990, AMPS, a first-generation cell phone standard, was the dominant US cell phone standard. But since then, AMPS was replaced by D-AMPS, GSM, CDMA2000, WiMax, and then 4G LTE technologies. The competition generated by cellular technologies has induced hundreds of billions of dollars in investment and consumer spending. This is a remarkable contrast to DSRC, which, despite the full support of the US government and the nominal support of dozens of auto and device companies, has generated marginal commercial interest.

Private companies see slow progress in many technical areas, and V2V technology poses unique technical issues. But private companies are subject to competitive pressures and consumer demands. A dead-end technology in the private sector is eventually shelved, and resources shift to promising (profitable) new developments. With government-mandated technology adoption, however, there are no competitive pressures and regulators are spending taxpayer money. As FCC's history shows—in obsolete technology standards like NTSC broadcast standards, FireWire, and CableCard—dead-end consumer technology that is mandated by government can live on, zombielike, for years or decades after the market has moved on.

Other Technologies Will Likely Overtake NHTSA's Mandated Devices

Prior predictions of DSRC deployment have been unreasonably optimistic. DSRC has failed to gain commercial traction, and the DOT appears to believe a mandate will save the federal government's sunk costs into DSRC. After assigning free spectrum for DSRC and codifying technology standards in 2004, the FCC believed there would be "rapid development and deployment of DSRC equipment." In January 2004, DOT officials told reporters they expected DSRC to be commercially available sometime in 2005. Yet, 12 years later, the DOT is still waiting for DSRC deployment.

The rapid development of cellular-based technologies poses the biggest competitive threat to DSRC. ITS proponents envisioned 32 different DSRC user services when DSRC spectrum was set aside in 1999. However, while ITS firms and the DOT have slowly developed DSRC, a robust wireless ecosystem of cellular technology, devices, and applications developed. Many of those 32 services have already been "solved" by non-DSRC technologies, including "map and music data updates," video uploads, parking lot payment, rollover warning, "driver's daily log," and "enhanced route planning and guidance." The DSRC V2V mandate is intended to provide drivers imminent collision warnings, but competing technologies like radar and lidar are already in the market. Automatic braking systems have been around for years, and research from the Insurance Institute for Highway Safety suggests that such systems are preventing more rear-end accidents than warning systems like the one NHTSA contemplates for its mandate.

Other technologies are improving fast and may prove superior to DSRC if the connected car market is permitted to develop. 3GPP, the global cellular standards body, for instance, released its initial V2X (vehicle to anything) standard in September 2016. In fact, as technology publications have reported, China is likely to use a cellular-based system, and Europe may follow. DSRC may prove to be a viable technology in other countries eventually, but it appears unlikely that, for instance, Japan or South Korea will mandate DSRC.

DSRC Is Not Safe and Reliable Today and May Fail to Be Roadworthy

The V2V network NHTSA is proposing to mandate is a mesh network, which means nodes communicate directly and without an intervening network. While mesh networks generated substantial academic interest circa 2000 when DSRC was developed, they have proven to be notoriously complicated and expensive to deploy. To my knowledge, aside from small experiments, there are no real-time communication mesh networks in existence. Perhaps predictably, researchers have found DSRC V2V units are subject to the reliability and resource management problems associated with mobile mesh networks.

It's important to allow the nascent connected car, V2V, and vehicle sensor markets to develop. DSRC is not safe and reliable today and has severe technical deficiencies that may or may not be remedied. The following draws from several researchers and engineers but especially from a Booz Allen Hamilton report produced for NHTSA in May 2016, referred to heretofore as the "Booz Allen Report."

DSRC Uses Legacy Technology That Is Ill-Suited for Vehicle-to-Vehicle Communications

The DOT proposes to mandate DSRC, which incorporates the IEEE 802.11p communications standard. Some of DSRC's reliability problems stem from IEEE 802.11 technology, which is also used in WiFi devices. The IEEE 802.11 standard was not designed for moving vehicles, and technology choices that are appropriate for home WiFi might not be appropriate for millions of moving vehicles. Researchers noted in a recent Institute of Electrical and Electronics Engineers journal article about DSRC's technical challenges that

"the typical use cases of IEEE 802.11 standards are sparse nomadic deployment with stationary channels. Consequently, existing commercial IEEE 802.11 chipsets are naturally optimized for best performance in such an environment. However, vehicular communications can happen among highly mobile vehicles, with multipath fading channel, and often in densely populated environments."

Further, different radio frequency bands have different transmission propagation characteristics. It's not clear that the 5.9 GHz band, assigned by the FCC in 1999 for DSRC, is optimized for V2V communications. Namely, as the DOT has acknowledged, non-line-of-sight transmissions suffer in the 5.9 GHz band.

Researchers have raised concerns for years about the reliability of DSRC transmissions under congested circumstances because DSRC has a relatively long range (at least 300 meters) but relatively narrow communications channels (10 MHz). NHTSA boasts of DSRC's range relative to competing systems, but extended range comes with downsides. With larger range, contention between vehicle device transmissions increases, and as researchers have found with DSRC simulations, larger ranges reduce the probability of channel access significantly.

In short, DSRC reliability plummets when many units are transmitting at the same time. The decision to have 10 MHz channelization for DSRC was chosen at an early stage in DSRC development. This decision was made because DSRC device makers could use existing, circa 2000, Wi-Fi chipsets. While this might have made sense 15 years ago, as Booz Allen and others have noted, 10 MHz channels underutilize the capability of current wideband technology. Namely, with 10 MHz channels, "channel congestion is a serious issue" and in dense traffic, "the occurrence of message losses" owing to congestion is "highly likely."

Booz Allen assessed how well DSRC units worked in a report for NHTSA. Their assessment is not encouraging. The Booz Allen Report goes on to note that the existing DSRC standards are "an inefficient use of the DSRC band" when used for V2V. This inefficiency means that even modest traffic can cause network congestion. "With perfect Carrier Sense Multiple Access (CSMA) performance," Booz Allen researchers said, "the system can support at most 204 vehicles transmitting BSMs at 10 Hz."

Another potential impediment to V2V effectiveness is how device updates are accomplished. DSRC units, like all mobile devices, will require periodic updates. The problem with a V2V-only network like the one NHTSA is proposing is that it doesn't have a pervasive, intervening network that can push updates. This flaw may be why the DOT's original DSRC plan was to deploy V2I networks first and V2V technology later. It is unclear to this researcher why the DOT's model changed over the years. It is premature to mandate DSRC V2V when it is unclear if updates can be effectively pushed to V2V units.

The Safety Pilot Model Deployment Reveals That DSRC Is Not a Reliable Anti-Collision Technology and May Never Be Safe for Mass Use

NHTSA grossly overstates DSRC's roadworthiness and underplays the serious upgrades needed before DSRC V2V devices are reliable and safe. For instance, NHTSA states that "DSRC is the only mature communication option that meets" the necessary requirements for collision avoidance and that it is effective at preventing potential crashes.

NHTSA points to real-world testing of DSRC in the Safety Pilot Model Deployment (SPMD), which purportedly "demonstrated the readiness of DSRC-based connected vehicle safety applications for

nationwide deployment." NHTSA says that the SPMD showed that DSRC V2V devices "have proven effective in mitigating or preventing potential crashes" and need only "additional refinement."

The truth is that the SPMD revealed serious problems with DSRC and had limited value in showing safety. The SPMD field tests were delayed, lasted only a few weeks, and were beset by technical problems. As NHTSA states in the NPRM, the deployment analysis was limited: it assessed "whether the prototypes and the system worked, but not necessarily how well they worked." The DOT noted that "every DSRC device deployed had to be recalled at least once during the SPMD to identify and correct issues." False alerts were a particular problem.

The Booz Allen analysts found that the DOT's 2014 Safety Pilot Model Deployment offered "relatively few vehicle interactions and no known identified situations where vehicles were on collision courses and the system properly warned the driver, or where vehicles were on a near miss course and the system accidentally warned the driver." With no known situations testing collision avoidance, the analysts used DSRC device parameters to simulate collision situations.

They identified "significant issues with the accuracy requirements on the data in the BSM [basic safety message]." The researchers found that "if the BSM data is only accurate to within the error tolerances stated for the Safety Pilot program, the system will be able to reliably predict collisions only about 35% of the time." The current error tolerances for DSRC V2V units, they added, "will fail to provide the desired levels of intended and reliable safety benefits."

Alarmingly, in simulations DSRC units misclassified vehicle interaction (i.e., a collision or miss) 72 percent of the time five seconds away from impact. The report noted that "the chance of a misclassification [of a collision or near miss] occurring, even at 1 second prior to collision, is concerning." Error rates improve as vehicles approach each other, but even one second before a sure collision, DSRC devices had only an 80 percent rate of detecting the collision. Since drivers need three or more seconds to respond to a collision warning, the researchers concluded the error rate "draws into question the safety integrity of the system."

The authors stated that "much tighter tolerances . . . are needed in order to assure data sent from vehicles can be used to reliably predict imminent collisions and generate driver warnings or other mitigation actions." These improvements, the team says frankly, "may be challenging to achieve." The researchers concluded:

"If the objective is that the system must not miss more than 5% of actual collisions, the resulting BSM parameter accuracy requirements will need to be much tighter. If the objective is 99.999% (0.001% classification failure) reliability, then the system is probably not viable."

Before mandating a specific V2V technology for light vehicles, NHTSA should first determine an acceptable collision rate. Without such, the agency may be mandating a technology that will never have acceptable reliability.

The agency proposes to require "that a message packet error rate (PER) is less than 10%." It is not clear that DSRC units satisfy this proposed standard. The Booz Allen analysis revealed significant signal degradation when dozens of DSRC units are in close proximity. They estimated that if 256 devices were in a 100 x 100 meter area, packet error rates would exceed 45 percent. Since heavy traffic of

DSRC-connected cars would mean 400 to 600 vehicles within range of a DSRC device, the mandated device specifications may be inadequately safe.

Devices Can Interoperate without a Mandate

NHTSA asserts that "without government intervention," V2V communications will not be standardized and interoperable. Scholars have found that the public sector is ill-suited to determine what specific technology will be the best option for the future, especially where complex information technologies are involved.

Mandating that other technologies have interoperability with DSRC, as NHTSA proposes, adds to the complexity. This may cause firms to shy away from wireless communications technologies. "Interoperable" means many things when it comes to DSRC V2V, and certification testing alone will take time—perhaps years—to develop and operationalize. Further, DSRC's design-by-committee framework requires compromises between powerful tech, auto, and government interests that likely sacrifices speed, performance, or both.

The existing communications market reveals that interoperability arises without a government device mandate. Market processes do create reliable and interoperable networks. Cellular phones, for instance, absent regulatory mandates, have both interoperable elements (SMS messaging, VoLTE) and non-interoperable elements (IP messaging, CDMA versus GSM, operating systems, app stores).

Interoperability for critical services can be quite rapid even without a mandate. Tens of thousands of computer networks connecting billions of devices, for instance, interoperate and exchange IP traffic without a mandate to interoperate. Firms interoperate because interoperability increases the value of a platform. Verizon introduced VoLTE, an inter-carrier voice communications technology, to subscribers in 2014. By early 2017, most Verizon voice traffic was transmitted via VoLTE. This is a remarkable example of a company developing an important application (voice) that interoperates across networks and across millions of devices.

NHTSA also proposes requiring non-DSRC technologies not merely to interoperate with DSRC technology when sending BSMs, but to have very similar technological characteristics. In effect, NHTSA is mandating DSRC-like requirements for non-DSRC V2V wireless technology. These constraints are limiting, particularly the proposed requirement that non-DSRC technologies have a minimum 300-meter range. Since this extensive range increases the chance for congestion, this requirement biases future technologies to low-throughput information. No one can be certain, ex ante, that the high-range, low-throughput applications NHTSA de facto requires will be more useful and lifesaving than low-range, high-throughput applications, or some other mix of capabilities.

Conclusion

DSRC V2V technology is far from roadworthy. Any technology "so good it must be mandated" warrants extreme skepticism. Many of DSRC's technical elements were mandated over a decade ago and underutilize current wireless technology. Researchers have pointed out that DSRC has many technical drawbacks and is unreliable. The Booz Allen Report concluded in 2016, a few months before the NPRM:

"Ideally, these technical issues would be resolved before finalizing requirements, but given the NHTSA rule-making timeline, it may not be possible for complete solutions to be included in the first rule."

Modifying the DSRC standards would bring operational benefits, especially regarding congestion, but would require yet another lengthy FCC rulemaking. Connected car and sensing technology is advancing rapidly. Given the dynamic marketplace, any connected car device mandate would not only be unprecedented, at this point in DSRC development, it would be dangerously hasty. The agency should halt this NPRM, resolve DSRC's many technical issues, and allow the connected car market to develop before proceeding.

Serious Privacy Risks Lie in the Path of Vehicle Automation
Center for Democracy and Technology Blog
Joseph Lorenzo Hall
April 13, 2017

Yesterday, CDT joined four top cryptography and security experts – Leonid Reyzin, Anna Lysyanskaya, Vitaly Shmatikov, and Adam D. Smith – in raising serious privacy concerns with proposed next-generation vehicle-to-vehicle communication standards (find our comments here).

The National Highway Traffic Safety Administration (NHTSA) has proposed a new standard – a Federal Motor Vehicle Safety Standard (FMVSS) – that details the messaging formats for communications between vehicles for future vehicle automation. While we raise concerns here, make no mistake: increased automation of land vehicles like cars and trucks holds great promise, from drastically reducing injuries and deaths in accidents to streamlining traffic in order to route vehicles in the most efficient ways possible. To do this, our vehicles will be increasingly talking to each other and to other infrastructure on the road such as traffic signals, signage, and lane boundaries in order to keep us safe. At the same time, in the race towards promising applications, we need to be careful that we don't introduce features that may reduce the trust and freedom we have in our vehicles.

It's clear that the current set of proposed standards fall short of what we need in a next-generation vehicle-to-vehicle (V2V) standard. In addition to our critique, other commenters like Alishah Chator and Matthew Green from John Hopkins University describe in their comments how the credential management system has a number of serious weaknesses.
In our comments, we point out that the Basic Safety Message (BSM) – a message broadcast ten times a second with granular data about position, speed, direction, and path history – poses serious privacy risks to drivers and passengers:

- The BSM must report location accuracy to 1.5m, sufficient enough to pinpoint the parking spot of a car or even the specific driveway or garage in a suburban environment where the car is located, allowing a specific vehicle to be linked to its BSM messages.
- The BSM includes a temporary ID and a security certificate that change every 5 minutes ostensibly to destroy any linkability; however, there is enough continuity between other data in the message – path history, speed, acceleration, and yaw – to link BSMs across a change in these credentials.
- If an observer misses one of these credential changes, other data like vehicle size (.2m precision in each dimension) or the inherent relationship among the speed, acceleration, steering angle, and yaw will vary subtly among different makes and models, helping to link a specific vehicle to its BSMs.
- The security certificates themselves can allow an observer to link BSM messages. A vehicle will at most have 20 of these certificates active each week and a car starting and stopping in

the same place (e.g., a driveway) will permit an observer to link most of a vehicle's weekly allotment of certificates to the same driveway and, thus, to the same vehicle.

Needless to say, we have serious concerns about the level of granular privacy leakage possible with the BSM message format in its current design. It's no exaggeration to say that this design makes it possible to track the entire vehicular movements of a neighborhood or small town with a single antenna and computer for under a few thousand dollars. While of course it's possible to follow vehicles physically, track them via GPS/cellular signals, or use license plate-reading cameras to follow their movements, none of these can be accomplished with such easily concealed, cheap tools that require no access to private infrastructure. We go on in the comment to discuss shortcomings in the privacy study for the proposed standard, pointing out that tools can be made much cheaper and more powerful than suggested in the privacy study, with only a bit of extra effort.

We call for this system to be explicitly opt-in or for the design to be significantly reconsidered so as to avoid the problems we identify. There are some promising tools from applied cryptography that could be leveraged to design a system that would impact driver and passenger privacy to a much lesser extent. Technologies such as anonymous tokens can give a vehicle the ability to send anonymously authenticated messages that have the property of removing anonymity – and revoking credentials – if the vehicle misbehaves. Further research in this area and a deeper engagement with the cryptography and privacy research communities are likely to yield a design that can give us the benefits of V2V communication without such devastating privacy costs.

Part of the difficulty here is that NHTSA has largely disclaimed any ability or interest in policing non-safety applications of V2V information, leaving the field open to unexpected commercial uses as well as privacy-invasive uses like those we discuss above. While we are hopeful that the standard could be improved to drastically reduce the current extent of privacy risks, we feel that NHTSA should be more engaged with entities like the Federal Trade Commission who have the authority and expertise to deal with non-safety privacy issues. And we are very glad to see the upcoming joint FTC/NHTSA workshop this summer which should be a perfect venue for further discussion of these risks and potential fixes.

Proceed With Caution
Morning Consult
Alex Kreilein
April 12, 2017

Vehicles designed in the grand era of the 1950s and '60s leaned toward the future. Many of those cars were brilliance in motion. But unlike today's cars, they weren't actually smart. Modern vehicles are essentially computers on wheels. Like all computer systems, vehicles are open to exploitation by hackers or even misconfiguration by their manufacturers. As such, we cannot take an old-school mentality when building new-school systems.

Noted researchers such as Charlie Miller, Chris Valasek, Craig Smith and Josh Corman have led the way in vehicle security by publicly addressing vulnerabilities in vehicles. Research by these experts and others prove that vehicles, like any other computer system, can be exploited by hackers. Yet, while their contributions have been widely recognized and supported in the security community, they do not seem to be meaningfully addressed by the automotive industry and government regulators.

The 2015 recall of certain Fiat-Chrysler Automotive models due to a critical systems vulnerability in the Harman-Kardon infotainment system proves that there is a problem. Attackers were able to remotely access the comfort and entertainment system and use it to gain unprivileged access to the critical control functions of the vehicle. But this isn't a Fiat-Chrysler problem alone. Security researchers were able to hack a 2014 Jeep Cherokee, leading to a 1.4 million vehicle recall. All of this proves that we know there is a problem, now we need to have the fortitude to fix it.

The National Highway and Transportation Safety Administration is about to wirelessly enable vehicles without taking steps to fully ensure that motorists are protected from cyberattack, making previously hard to access vulnerabilities exploitable over wireless systems. More than this, NHTSA will ensure that mission-critical functions supporting life and safety share the same communications links with commercial applications that support monetization. It's time we wake up and address this.

By integrating wireless communications systems into vehicles without first addressing the current and future vulnerabilities of vehicles, and requiring that significant countermeasures and mitigations be in place, NHTSA and the automotive manufacturers are about to put lipstick on a pig and tell you it's pretty. The sad part is that regulators know what they're doing and no one is paying attention enough to stop them.

The protocol known as Dedicated Short-Range Communications cannot compensate for the known and unknown vulnerabilities of vehicles themselves. In fact, DSRC will make it easier for attackers to exploit those vulnerabilities. While NHTSA-proposed rules for cryptography may address certain attack methods, cryptography alone cannot possibly compensate for the host of vulnerabilities that we know about today and those we can only imagine in the future. Because of this, attackers are about to get a free ride at your expense. This is a bad deal for consumers, taxpayers, motorists and companies.

Connected vehicles enabled with DSRC are vulnerable to at least six specific categories of attacks: deception attacks; denial of service attacks; cryptographic exploitation; malware exploitation; jamming and spoofing; and V2X exploitation. To ensure that we do not inadvertently transform connected vehicles into mobile malware delivery systems and risk both our safety and privacy, it is incumbent on policymakers and automotive manufacturers to set clear rules for the deployment of connected vehicles.

NHTSA must require a transparent vehicle security framework and compliance mechanism. Consumers have the right to know if their vehicles are safe. Government has a responsibility to ensure that every make and model of connected vehicle is reasonably safe. Automotive companies have the right to innovate but must ensure security. Without all of this, security becomes a race to the bottom, where the tragedy of the commons rules the road. An industry-led framework with light oversight ensures that the rules of the road are followed but that innovation is promoted.

Cybersecurity is a first order consideration. All of the good stemming from the innovations of automotive companies can be quickly undone if people do not trust the product, if hackers easily win and if we do not address risk. Without addressing the way vehicles are secured today, we cannot safely put the brilliance of connected vehicles in motion. In order for America to realize the promise of a connected society, we must make security a priority.

Public Knowledge Files NHTSA Comments Raising Safety, Privacy Concerns with DSRC Technology
Public Knowledge Blog

Shiva Stella
April 12, 2017

Today, Public Knowledge, Consumer Federation of America and New America's Open Technology Institute submitted comments to the National Highway Traffic Safety Administration's Notice of Proposed Rulemaking on mandating Direct Short Range Communication (DSRC) service for vehicle-to-vehicle (V2V) communications.

The NPRM seeks to examine ways to reduce the number and severity of motor vehicle crashes in the United States. Public Knowledge supports this goal but advises against commercializing the DSRC service, which would leave the door open for non-safety uses of DSRC spectrum, introducing unresolved cybersecurity risks and consumer privacy concerns.

The following can be attributed to John Gasparini, Policy Fellow at Public Knowledge:
"We are reiterating our concerns about NHTSA's DSRC mandate for all new cars in this filing. In recent months, we've seen a dramatic increase in consumer interest in privacy and cybersecurity protections. While consumers clamor for greater protections, however, NHTSA continues advancing a proposal that would mandate a vehicular technology that not only lacks adequate privacy or cybersecurity protections but also remains open to commercial use.

"This cybersecurity approach lacks depth, opening the door to additional threats to all cars and expanding attack vectors into already-vulnerable vehicles. On privacy, NHTSA goes further, washing its hands of any concerns about data collection or data use by third parties. This is particularly problematic when we're talking about mandatory technology that could be used to track individual cars -- and their drivers.

"This is made more troublesome because NHSTA's proposal leaves the door wide open for commercial services like infotainment, advertising, and social media platforms. Deploying commercial services like Facebook, mobile payments and targeted advertising in automobiles only amplifies DSRC's cybersecurity risks. If this mandate is truly about safety and saving lives, it should focus exclusively on those goals and close the door to commercial interests that aren't about safety until the cybersecurity and privacy concerns are adequately addressed.

"The digital revolution of recent decades shows no sign of slowing down, but we must not let enthusiasm for progress impede network security best practices. Although we support efforts to leverage technology to make cars safer, we are concerned that the current proposal causes more problems than it solves. When it comes to ensuring safety in a landscape of increasingly complex technologies, the duty to consumer safety and security must always come first. While NHTSA and the auto industry are in the driver's seat, we urge them to please drive safely."

You may learn more about DSRC technology here. You may also view this full release.

CEI Submits Comments on Proposed Vehicle-to-Vehicle Communications Mandate
Competitive Enterprise Institute
Marc Scribner
April 12, 2017

Today, CEI submitted comments to the National Highway Traffic Safety Administration (NHTSA) in response to its notice of proposed rulemaking (NPRM), "Federal Motor Vehicle Safety Standards; V2V Communications," which was published in the Federal Register on January 12, 2017. In it, NHTSA proposes to mandate that all new light-duty vehicles have vehicle-to-vehicle (V2V) communications devices installed and that they use a particular communications protocol called dedicated short range communications (DSRC). The purpose of the mandate, as currently contemplated by NHTSA, is to offer future drivers advance warnings of traffic and roadway hazards.

Last week, CEI and a coalition of free-market organizations sent a letter to Secretary of Transportation Elaine Chao asking her to temporarily suspend the V2V rulemaking proceeding in order to allow the new administration to examine this controversial midnight Obama proposal. CEI previously submitted comments in 2014 in response to NHTSA's advance notice of proposed rulemaking on V2V.

The full comment letter is here. We develop four points, which are summarized below.
First, NHTSA fails to adequately consider alternatives to DSRC, ones that could enable faster adoption of V2V at a lower cost. Wireless carriers plan to upgrade their networks to next generation mobile networks, known as 5G, over the same time period as the mandate phase-in, which resolves many of the latency (delay) issues with earlier cellular-based V2V while harnessing existing terrestrial networks—meaning there would be no need to install nearly 20,000 roadside devices along the National Highway System to support the mandated V2V-DSRC system. Moreover, NHTSA does not explain who would pay for this new infrastructure or how it would be funded and maintained.

Second, NHTSA leaves a number of important privacy and cybersecurity issues unresolved. The agency proposes a Secure Credential Management System (SCMS) to mitigate these risks but does not propose any specific regulatory text. This is worrying because the SCMS would be a critical component of safely functioning V2V. NHTSA, at the very least, should propose SCMS regulatory language prior to the promulgation of a final rule and allow the public to examine and comment on it.

Third, NHTSA's plan to require owner consent for software updates and new security certificates undermines the claimed benefits of forced V2V. While the agency is not inclined to allow automakers to install V2V devices with an "off switch" for drivers wishing to disable V2V, V2V can nonetheless be disabled under NHTSA's proposal if the owner refuses updates. NHTSA suggests that a telltale lamp or dashboard message could prod drivers to consent to updates, but this likely will not deter some drivers from allowing their V2V devices to deactivate. Given perceived (and real) privacy and cybersecurity risks, and the fact that around 10 percent of vehicles on the road today display "check engine" telltales, NHTSA should better consider the "apathy rate" in its benefits projections.

Fourth, NHTSA fails to adequately consider the impacts of forced V2V on vehicle automation systems. Automation has the potential to save far more lives than V2V hazard warnings, but requiring a one-size-fits-all approach to connectivity introduces new privacy and cybersecurity risks into these automation systems. This is the reason most automated vehicle developers are focusing exclusively on vehicle-resident sensor technologies, rather than connectivity. It has been argued by a number of developers and technologists that V2V-DSRC as contemplated by NHTSA is obsolete, and that requiring all new vehicle—included automated vehicles—to come installed with V2V devices puts these new, more promising technologies at risk.

Based on these concerns, we conclude by urging NHTSA to withdraw the NPRM. Read the full comment letter here.

Protect Your Privacy and Save Money by Telling NHTSA No to the Vehicle-to-Vehicle Communications Mandate

CATO at Liberty
Randal O'Toole
April 5, 2017

Comments on the National Highway Traffic Safety Administration's proposed vehicle-to-vehicle communications mandate are due next on Wednesday, April 12. This is one of the rules that was published just before President Trump was inaugurated. If approved, it will be one of the most expensive vehicle safety rules ever, adding around $300 dollars to the price of every car, or (at recent car sales rates) well over $5 billion per year.

Despite the high cost, the NHTSA predicts the rule will save no more than 31 lives in 2025, mainly because it will do little good until most cars have it. Yet even by 2060, after consumers have spent well over $200 billion so that virtually all cars would have it, NHTSA predicts it will save no more than 1,365 lives per year.

The danger is not that it will cost too much per life saved but that mandating one technology will inhibit the development and use of better technologies that could save even more lives at a lower cost. The technology the NHTSA wants to mandate is known as dedicated short-range communications (DSRC), a form of radio. Yet advancements in cell phones, wifi, and other technologies could do the same thing better for less money and probably without a mandate.

For example, your smartphone already has all the hardware needed for vehicle-to-vehicle communications. Since more than three-fourths of Americans already have smartphones, mandating similar technology in new cars is redundant. Since that mandate will take more than a decade to have a significant impact on highway safety, NHTSA could see faster implementation using smartphones instead. It could do so by developing an app that could communicate with cars and provide extra features on the app that would encourage people to download and use it.

All of the benefits claimed for the DSRC mandate assume that no other technology improvements take place. In fact, self-driving cars (which will work just as well with or without vehicle-to-vehicle systems) will greatly reduce auto fatalities, rendering the projected savings from vehicle-to-vehicle communications moot.

A mandate that one technology be used in all cars also opens the transportation system to potential hackers. The communications would necessarily be tied to automobile controls, which means that anyone who understands it could take control of every car in a city at once. If individual manufacturers were allowed to develop their own technologies, the use of multiple systems would make an attack both more difficult and less attractive.

There is also a privacy issue: vehicle-to-vehicle also means infrastructure-to-vehicle communications, raising the possibility that the government could monitor and even turn off your car if you were doing something it didn't like, such as drive "too many" miles per year. That's a very real concern because the Washington legislature has mandated a 50 percent reduction in per capita driving by 2050. Oregon and possibly other states have passed similar rules.